5-2016

STANDARDIZING FUNCTIONAL SAFETY ASSESSMENTS FOR OFF-THE-SHELF INSTRUMENTATION AND CONTROLS

Andrew Michael Nack
University of Tennessee - Knoxville, anack@vols.utk.edu

To the Graduate Council:

I am submitting herewith a thesis written by Andrew Michael Nack entitled "STANDARDIZING FUNCTIONAL SAFETY ASSESSMENTS FOR OFF-THE-SHELF INSTRUMENTATION AND CONTROLS." I have examined the final electronic copy of this thesis for form and content and recommend that it be accepted in partial fulfillment of the requirements for the degree of Master of Science, with a major in Computer Engineering.

Gregory D. Peterson, Major Professor

We have read this thesis and recommend its acceptance:

Qing C. Cao, Mingzhou Jin

Accepted for the Council:
Carolyn R. Hodges

Vice Provost and Dean of the Graduate School

(Original signatures are on file with official student records.)

STANDARDIZING FUNCTIONAL SAFETY ASSESSMENTS FOR OFF-THE-SHELF INSTRUMENTATION AND CONTROLS

A Thesis Presented for the
Master of Science
Degree
The University of Tennessee, Knoxville

Andrew Michael Nack
May 2016

ACKNOWLEDGEMENTS

Thank you to my wife Leslie, my kids Jerrett, Mikie, Elijah, and Anna Bowden, my advisor Dr. Gregory Peterson, my committee members Dr. Charles Cao, and Dr. Mingzhou Jin, my unofficial committee member Dr. Richard Wood, my friend Dr. M. Nance Ericson, my new friend Gary Johnson, my previous and current bosses Matthew Bowman, and Milton Concepcion, and my employer ATC Nuclear. I received critical support from all these people and entities, and I would not have been able to be successful without them.

ABSTRACT

It is typical for digital instrumentation and controls, used to manage significant risk, to undergo substantial amounts of scrutiny. The equipment must be proven to have the necessary level of design integrity. The details of the scrutiny vary based on the particular industry, but the ultimate goal is to provide sufficient evidence that the equipment will operate successfully when performing their required functions.

To be able to stand up to the scrutiny and more importantly, successfully perform the required safety functions, the equipment must be designed to defend against random hardware failures and also to prevent systematic faults. These design activities must also have been documented in a manner that sufficiently proves their adequacy.

The variability in the requirements of the different industries makes this task difficult for instrumentation and controls equipment manufacturers. To assist the manufacturers in dealing with these differences, a standardization of requirements is needed to facilitate clear communication of expectations. The IEC 61508 set of standards exists to fulfill this role, but it is not yet universally embraced. After that occurs, various industries, from nuclear power generation to oil & gas production, will benefit from the existence of a wider range of equipment that has been designed to perform in these critical roles and that also includes the evidence necessary to prove its integrity. The manufacturers will then be able to enjoy the benefit of having a larger customer base interested in their products.

The use of IEC 61508 will also help industries avoid significant amounts of uncertainty when selecting commercial off-the-shelf equipment. It is currently understood that it cannot be assumed that a typical commercial manufacturer's equipment designs and associated design activities will be adequate to allow for success in these high risk applications. In contrast, a manufacturer that seeks to comply with IEC 61508 and seeks to achieve certification by an independent third party can be assumed to be better suited for meeting the needs of these demanding situations. Use of these manufacturers help to avoid substantial uncertainty and risk.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE

INTRODUCTION AND GENERAL INFORMATION

Industries that utilize digital instrumentation and controls equipment to manage significant risk must overcome many hurdles that other industries do not encounter. Because of these significant risks, the nuclear industry, the defense industry, and some of the process industries go to great lengths to ensure their facilities operate safely and reliably. These efforts cause instrumentation and controls equipment manufacturers to have levels of requirements imposed on them that are much more demanding and rigorous than what they typically experience. As should be expected, such equipment is subject to considerable price increases and significant delivery time delays.

In these cases, digital commercial off-the-shelf (COTS) equipment is being evaluated and utilized for safety applications. Typically these evaluations occur on a case-by-case, application-specific basis. It would be advantageous to users and producers of the equipment if these evaluations could move towards being more generic and standardized. If other industries understand the criteria utilized in that original evaluation they may be able to leverage it and eliminate redundant effort towards their own similar evaluations. If multiple high risk industries can utilize some of the same off-the-shelf equipment and the same evaluations it will likely result in a mutually beneficial situation for all members involved. The manufacturer will be able to become proficient at dealing with these industries' non-typical requirements and also distribute the cost of their extra effort to a larger customer base. At the same time, the industry equipment users will benefit from manufacturers who are more effective with meeting their technical and quality related needs, and will benefit from the manufacturer being able to provide this type of equipment at lower prices. Basically the industries will get better equipment at better pricing while the manufacturer gets more customers that want the products they are selling, with a minimal increase in oversight activities such as audits and external design reviews.

To achieve this goal, there are many details that must be worked out. The industries must understand each other in how they are different and how they are the same. The criteria for these comparison include how classification of equipment is handled, how random failures are defended against, how systematic faults are prevented, and how off-the-shelf equipment is evaluated for suitability. This knowledge is critical to understand when evaluations and operating experience can be extrapolated and when they cannot. Another detail is that a vehicle of standardization must be in place between the industries and the manufacturers to clearly communicate the expected safety and reliability targets. The level of rigor can vary greatly within these topics, especially when software development is involved, so standardizing what is expected is crucial in order to avoid great frustration from both the industries' perspective and the manufacturer's perspective. The technological advances of computer-based

equipment have been significant in recent years, and hold great promise in their value to users. But at the same time, the increase in complexity of individual components has considerably increased the effort and level of difficulty involved in performing the evaluations for confirming suitability.

In order to deal with many of these details a process of certifying equipment to meet IEC 61508 Functional Safety Standards has been established. At this point in time, it is a widely under-utilized process and holds great potential as it becomes better understood and more widely implemented. IEC 61508 provides insight both for the industries using the safety systems and also for the manufacturers designing and building the equipment. The goal of this thesis is to make this potential better understood and also to provide some examples of how it can be accomplished.

Planning to use commercially developed, digital, COTS equipment in safety systems is criticized in some industries as being a very risky and unpredictable endeavor. The US Department of Defense (DOD) identifies these risks as being:

- *Potential for limited development, test, or configuration control documentation*
- *Unknown development history (standards, quality assurance, test, analysis, failure history, etc.)*
- *Unavailability of design and test data (drawings, test cases and procedures, test results, etc.)*
- *Proprietary design prohibitions*
- *Unable to modify based on limited proprietary or data rights*
- *Unknown functionality and functional limitations (operational, environmental, stress, etc.)*
- *Limited or no supportability from the developer or vendors (configuration control, tech support, updates, etc.)*
- *Unnecessary functionality or capabilities (the potential of "hidden" or undocumented functionality)*
- *Potential obsolescence of the COTS application*
- *May not be developed to best industry or Government practices or certification criteria*
- *Unavailability of safety analyses for the COTS application*
- *Potential for increased test and analysis required for safety verification, safety release, or safety certification*
- *Potential need for periodic updates and the unknown impact of those updates*
- *Functions or tasks unneeded by the intended program*
- *Unable to modify due to licensing requirements, or the purchase of the license agreement* [1]

The US nuclear industry also makes the following statements about the prospect of using digital COTS equipment, "Make sure you understand what you're signing up for when you decide to go with a commercial product [2]," and "Be careful with

cost/benefit assessments. The evaluation and acceptance activities can easily cost far more than the digital device [2].” There is a general understanding that very little can be assumed about the characteristics of the designing and manufacturing processes of a commercial manufacturer. They may or may not have a formal and documented quality assurance program. They may or may not implement a structured hardware and software design process. They may or may not evaluate the reliability of their products. They may or may not perform and document verification and validation activities of their hardware and software designs. They may or may not take adequate steps to prevent systematic design flaws from being present in their equipment. All of these factors contribute to the recognized risk of using digital COTS equipment.

This thesis will focus on two points. The first point is the need for standardization of functional safety requirements. This is important for clear communication of expectations between various industries and equipment manufacturers. Also, the case will be made for IEC 61508 as being that necessary standard. The second point will be to demonstrate that many of the risks associated with the selection of COTS equipment can be mitigated by using commercial vendors who have pursued IEC 61508 safety integrity level (SIL) certification of their products. The results of this thesis will show that when a manufacturer’s product is certified as being SIL 2 or higher by a trusted third party it becomes reasonable to make some assumptions about the adequacy of the design and manufacturing processes that the manufacturer is implementing.

Other issues such as technology obsolesce and counterfeit parts are acknowledged to be relevant to the manufacturing processes of commercial equipment, but will not be expanded on as part of this work. Instead, the focus will be on the evaluation of suitability in terms of the design and related design processes of the equipment. There is certainly sufficient scope of concerns for the manufacturing processes to warrant future work in that area, but it is thought to be most impactful to focus on the design aspects at this point in time.

There are a couple of additional notes that should be mentioned. First, the author of this thesis has a natural bias towards the nuclear industry since that is where most of his work experience is from. An attempt will be made to broaden observations and viewpoints to apply to a wider scope. Second, it is critical to understand that discussions of instrumentation and controls equipment should be interpreted as embedded computer systems, where both hardware and software (aka firmware) are required to function correctly for the overall device to function correctly. Third, the topics of reliability and correctness of equipment is split into two separate discussions, throughout this thesis, because some types of equipment failures occur without the failure of any hardware subcomponents. All of the subcomponents could be reliable but the equipment could still fail. In these situations the failure is due to a lack of correctness and not due to poor reliability. A lack of correctness is what will often be referred to as a systematic fault.

The format of this paper is that chapter two provides an overview of the literature review focusing on establishing the originality of this work. Chapter

three expands on the literature review of the industry specific laws, standards, and guides to provide insight into how each handles safety system equipment. Chapter four identifies the relevant similarities and differences between these industries to provide insight into how they can work together and how they cannot. The existence of similarities between the industries provides evidence in the value of uniting behind a standardization of functional safety requirements to interact with equipment manufacturers. Chapter five presents examples of digital COTS equipment that has been certified to SIL level 2 or higher. The examples use publically available literature to show that it is reasonable to expect a higher level of rigor in the design of equipment from these manufacturers who have achieved these ratings from independent and trusted third party evaluators.

CHAPTER TWO

LITERATURE REVIEW

A literature review was performed with the initial purpose of ensuring that existing work and knowledge in this subject matter area was utilized and to also ensure this effort was an original work, not duplicating existing efforts. To this end, the following databases were searched: IEEE Explore, IAEA- INIS, DODSSP (Dept. of Defense Single Stock Point) [Assistdocs.com], and Google Scholar. Table 2.1 contains the most relevant results. Several useful resources were identified and it was confirmed the planned new work would be an original effort.

The second purpose of the literature review was to gather laws, standards, and guidance from industries that utilize digital instrumentation and controls equipment to manage significant risk and develop an understanding of how each industry handles safety system equipment. Four specific aspects of each industry were included in these industry reviews. Those categories are classification of systems and components, defending against random failures, preventing systematic faults, and suitability evaluations of off-the-shelf equipment.

The IEC 61508 standard was included in these categorical literature reviews as a non-industry specific reference. Regarding the topic of classification, the IEC 61508 safety integrity levels (SILs) are not actually a part of a classification methodology and therefore have been excluded from Table 2.2. SILs are described in more detail in chapter three, but in summary, they are an indicator of the design integrity of the certified equipment and the associated design activities.

Additionally Table 2.3 addresses random failures and Table 2.4 addresses systematic faults. Table 2.5 addresses the suitability evaluations of off-the-shelf equipment, but several terms are necessary to be understood to trace this topic through the identified documents. The actual evaluation is referred to as a proven in use evaluation, a prior use evaluation, suitability evaluation, or commercial grade dedication. The equipment involved is referred to as pre-existing, pre-developed, commercial grade, COTS, or non-developmental items. These terms should be considered as interchangeable and the text of this thesis will trend towards the use of suitability evaluation and off-the-shelf equipment. There are exceptions since sometimes it is helpful to use the terminology that matches the particular context, but when those occur understand these to refer to the same topic.

Table 2.1. Most Similar Works
The documents in this table are the most similar works identified that are related to the comparison of industries that mitigate significant risk using digital instrumentation and controls equipment

Existing Work	Summary of Evaluation
Nuclear Use of I&C Equipment Certified for Commercial Safety Use [3] Author: Gary Johnson	This was a high level presentation but identifies some of the core ideas this new work is focused on calling attention to and demonstrating. This new work is intended to do some of the tasks that this presentation called for.
Comparison of IEC and IEEE standards for computer-based control systems important to safety [4] Author: Gary Johnson	This was very relevant and very helpful information that I used as foundational work for my literature comparison work. It did not use the same categories of comparison, but it is a more comprehensive look at the two nuclear frameworks.
US NRC NUREG/CR-7007 Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems [5] Author: Richard T. Wood	In an effort to better understand common cause failures, several non-nuclear industries were researched to determine best practices. The new work is intended to loosely follow this model in an effort to focus on the topic of off the shelf equipment.
Comparison of the Software Safety Criteria between IEC and IEEE Standards for the Digital Instrumentation and Control System [6] Authors: Jang-soo Lee, Kee-choon Kwon	This work appeared to be very relevant but was very high level. It described an on-going effort without much detail. An effort was made to find a follow-up paper that might provide better detail but none was found.
Software Safety and Reliability- Techniques, Approaches, and Standards of Key Industrial Sectors [7] Author: Debra S. Herrmann	Presented concepts of both safety and reliability and explains the difference between the terms. It provides good basic background information for various industries where instrumentation and controls equipment is used to mitigate significant risk. This work did not perform any comparisons related to the topics addressed in this new work.
A methodology for evaluating, comparing, and selecting software safety and reliability standards [8] Author: Debra S. Herrmann	This work was focused on the selection of safety standards from the perspective of the US FDA 20 years ago. There were some interesting insights but was not overall relevant to this new work due to its focus and age.
The potential for a generic approach to certification of safety critical systems in the transportation sector [9] Authors: Y. Papadopoulos, John A. McDermid	The concept was similar to this new work but the focus was on railway, automotive and aerospace sectors. This new work was planned to include nuclear power plants and it was not expected that there would be much instrumentation and controls equipment shared between transportation and nuclear power generation industries. Therefore this work was not considered very relevant to this new work.

Table 2.2. Documents Regarding Classification

The documents identified in this table address the topic of the classification of systems and equipment for the specified industries.

Process Industry	US (IEEE) Nuclear	International (IEC) Nuclear	US Department of Defense
• ISA 84.00.01 Part 3 [10]	• IEEE 603 Criteria for Safety Systems [11]	• IAEA SSG-30 Safety Classification [12] • IEC 61226 Classification [13]	• MIL-STD-882E Standard Practice for System Safety [14] • Joint Software Systems Safety Engineering Handbook [1]

Table 2.3. Documents Regarding Random Failures

The documents identified in this table address the topic of random failures for the specified industry and the non-industry specific standards

Non-Industry Specific	Process Industry	US (IEEE) Nuclear	International (IEC) Nuclear	US Department of Defense
• IEC 61508 Part 2 [15]	• ISA 84.00.01 Part 1 [16]	• IEEE 603 Criteria for Safety Systems [11] • IEEE 7-4.3.2 Criteria for Computers in Safety Systems [17] • IEEE 379 Single Failure Criterion [18] • IEEE 577 Reliability Analysis in Design and Operation [19] • IEEE 352 Principles of Reliability Analysis [20]	• IAEA SSR-2/1 Safety of Nuclear Power Plants: Design [21] • IEC 61513 General Requirements [22] • IEC 60987 Computer Based Hardware [23]	• MIL-STD-882E Standard Practice for System Safety [14] • Joint Software Systems Safety Engineering Handbook [1]

Table 2.4. Documents Regarding Systematic Faults
The documents identified in this table address the topic of systematic faults for the specified industry or non-industry specific standard

Non-Industry Specific	Process Industry	US (IEEE) Nuclear	International (IEC) Nuclear	US Department of Defense
• IEC 61508 Part 2 [15] • IEC 61508 Part 3 [24]	• ISA 84.00.01 Part 1 [16]	• IEEE 603 Criteria for Safety Systems [11] • IEEE 7-4.3.2 Criteria for Computers in Safety Systems [17]	• IAEA NS-G-1.3 I&C Systems Important to Safety • IEC 61513 General Requirements [22] • IEC 60987 Computer Based Hardware [23] • IEC 60880 Category A Software aspects [25] • IEC 62138 Category B or C Software aspects [26]	• MIL-STD-882E Standard Practice for System Safety [14] • Joint Software Systems Safety Engineering Handbook [1]

Table 2.5. Documents Regarding Suitability Evaluations of COTS
The documents identified in this table address the topic of suitability evaluations of COTS equipment. Common terms to be familiar with is commercial graded dedication (CGD), proven in use, and prior use.

Non-Industry Specific	Process Industry	US (IEEE) Nuclear	International (IEC) Nuclear	US Department of Defense
• IEC 61508 Part 2 [15]	• ISA 84.00.01 Part 1 [16]	• EPRI NP-5652 R1 Guidance for CGD [27] • EPRI TR-106439 Guidance for CGD of Digital Equipment[28] • EPRI TR-107339 Guidance for CGD of Digital Equipment[2] • EPRI 1011710 Handbook for Critical Digital Reviews[29] • IEEE 7-4.3.2 Criteria for Computers in Safety Systems [17]	• IEC 61513 General Requirements [22] • IEC 60987 Computer Based Hardware [23] • IEC 60880 Category A Software aspects [25] • IEC 62138 Category B or C Software aspects [26] • IEC 62671 Selection of Industrial Digital Devices of Limited Functionality [30]	• MIL-STD-882E Standard Practice for System Safety [14] • Joint Software Systems Safety Engineering Handbook [1]

CHAPTER THREE

MULTI-INDUSTRY SURVEY

Process Industries

For process industries such as chemical and oil & gas, the regulatory framework is not as defined as for others such as the nuclear industry. These industries have taken the initiative to create standards for functional safety and unite behind their implementation. The reason for taking the initiative is to avoid or delay government regulation by demonstrating that regulation is not needed. The perception (and possibly the reality) is that governments move to regulate industries in response to the general public perceiving “alarming” associated risks [31]. The main standard that was created to address the full lifecycle of safety instrumented systems (SIS) was IEC 61508 [32]. Another standard that is derived from IEC 61508, specifically for the process industries, is ISA 84.00.01(IEC 61511) [10], [16], [33]. Despite these self-initiated efforts, regulation does exist for many of these process industries and an example of acceptance of the industry standards can be found from OSHA who sent a letter to ISA in 2000 identifying, “ANSI/ISA-84.01-1996 as ‘a recognized and generally accepted good engineering practice for SIS’ and that if a company is in compliance with the standard ‘the employer will be considered in compliance with OSHA PSM requirements for SIS’” [31].

Concerning regulation of the oil and gas industry, there has become to be an extensive list of regulators involved that all seem to be staking out their own territory. Here is a list that was reviewed of these regulators:

Environmental Protection Agency (EPA)
Main responsibilities. *The EPA has primary responsibility for enforcing many of the environmental statutes and regulations of the US.*

Bureau of Land Management (BLM)
Main responsibilities. *The BLM manages vast stretches of public lands that have the potential to make significant contributions to the US' renewable energy portfolio. The BLM also manages federal onshore oil, gas and coal operations that make significant contributions to the domestic energy supply as the US transitions to a clean energy future.*

Bureau of Safety and Environmental Enforcement (BSEE)
Main responsibilities. *BSEE works to promote safety, protect the environment, and conserve offshore resources through regulatory oversight and enforcement.*

Bureau of Ocean Energy Management (BOEM)

Main responsibilities. *The BOEM manages the exploration and development of the nation's offshore resources. It seeks to appropriately balance economic development, energy independence, and environmental protection through oil and gas leases, renewable energy development and environmental reviews and studies.*

Federal Energy Regulatory Commission (FERC)
Main responsibilities. *FERC is an independent agency that regulates the inter-state transmission of electricity, natural gas, and oil. FERC also reviews proposals to build LNG terminals and inter-state natural gas pipelines as well as licensing hydropower projects.*

Pipeline and Hazardous Materials Safety Administration (PHMSA)
Main responsibilities. *PHMSA's mission is to protect people and the environment from the risks inherent in transportation of hazardous materials, including oil and gas.* [34]

Later in the survey of the international nuclear industry, IEC 61508 [32] is mentioned as being the parent document to the nuclear standard IEC 61513 [22]. That is because IEC 61508 is technically considered an industry independent standard. It was originally written to be used as a starting point for all industries that utilized safety systems. IEC 61508 is generally viewed as a standard that can be voluntarily adopted by equipment manufacturers to use in the design of new equipment intended for use in functional safety applications. Since the process industry closely adopted the requirements, guidance, and methodologies of IEC 61508 it will be surveyed here. Then a closer look will be taken at ISA 84.00.01(IEC 61511) [10], [16], [33] to review the process industry's specific implementations.

IEC 61508

This standard is a seven part document. Those parts are general requirements (part 1) [32], requirements for electrical/electronic/programmable electronic safety-related systems (part 2) [15], software requirements (part 3) [24], definitions and abbreviations (part 4) [35], examples of methods for the determination of SILs(part 5) [36], guidelines on the application of IEC 61508-2 and IEC 61508-3 (part 6) [37], overview of techniques and measures (part 7) [38]. This survey focuses on parts 1, 2, and 3 as they are the core of the requirements.

The IEC 61508 standard is laid out to explicitly specify the use of a life cycle methodology for the design, operation, and maintaining of safety systems. Part 1 describes the life cycle for overall plant safety. The overall plant life cycle phases are concept, overall scope and definition, hazard and risk analysis, overall safety requirements, safety requirements allocation, overall planning, safety systems realization, overall installation and commissioning, overall safety

validation, overall operation maintenance and repair, overall modification and retrofit, and decommissioning or disposal.

Part 1 also defines the use of SILs as an indicator of the level of rigor that went into establishing the integrity of the design of the equipment. The higher the SIL the higher the reliability targets are and the more rigorous the requirements are for the associated design process. The standard lays out the use of four SILs. SIL 1 is defined as $\geq 10^{-2}$ to $< 10^{-1}$ average probability of a dangerous failure per hour, SIL 2 is $\geq 10^{-3}$ to $< 10^{-2}$, SIL 3 is $\geq 10^{-4}$ to $< 10^{-3}$, and SIL 4 is $\geq 10^{-5}$ to $< 10^{-4}$ for low demand mode of operation. For high demand or continuous mode of operation, SIL 1 is defined as $\geq 10^{-6}$ to $< 10^{-5}$ average probability of a dangerous failure per hour, SIL 2 is $\geq 10^{-7}$ to $< 10^{-6}$, SIL 3 is $\geq 10^{-8}$ to $< 10^{-7}$, and SIL 4 is $\geq 10^{-9}$ to $< 10^{-8}$. The standard also acknowledges that these quantitative definitions focus on random hardware failures and are not directly relatable to systematic faults. It is further stated that it is necessary for additional qualitative definition to be added to the SIL levels in order to make them fully implementable[32].

Part 1 is focused on high level programmatic issues and points to parts 2 and 3 to address specific requirements for the realization of the actual hardware and software that make up the equipment used to implement the safety systems.

Part 2 of IEC 61508 [15] is focused on requirements for hardware and covers design measures for defending against both random failures and systematic faults. Part 2 also continues the embracing of the implementation of the lifecycle approach for hardware and identifies how Part 2 defines the realization phase mentioned in Part 1 with a much greater level of detail. The phases covered by Part 2 are safety requirements specification, safety validation planning, design and development (software is covered in Part 3 [24]), integration, installation commissioning operation and maintenance procedures, safety validation. These phases are intended to be specific to a certain safety system. Each safety system being realized will move through these phases independent of other safety systems.

The specification of the safety requirements phases is intended to be comprehensive. Beyond the expected functionality requirements, it is also expected that compatibility for the expected environmental extremes will be addressed (including electromagnetic compatibility). Typically the expected environmental extremes will encompass process industry parameters but does not make an effort to cover all possible extremes for other industries, such as nuclear power generation. Also hardware reliability goals corresponding to the SILs should be specified [15].

Several methods are identified as being potentially utilized to model/analyze hardware reliability. Those methods included cause consequence analysis, fault tree analysis, Markov models, and reliability block diagrams. These methods are how quantitative reliability goals can be shown to be achieved [15].

Another aspect of the life cycle process implementation worth noting is the use of verification and validation methodologies for the hardware. Sometimes this

methodology is only applied to software to ensure it meets its design requirements but it does make sense to utilize it for hardware also. It is a very practical approach to ensure requirements are being met. And for further clarification, the final validation of the hardware is performed with any associated software loaded into the programmable devices. This allows for functional requirements of the system to be more thoroughly validated in a manner that proves the hardware and software work together properly [15].

The appendices of Part 2 address issues related to detecting and controlling failures (random and systematic) during operation of the safety system and avoiding failures during different phases of the life cycle. Appendix A identifies a wide range of methods for achieving high levels of diagnostic coverage within the system hardware to ensure failures are identified and that no unsafe conditions are allowed to go undetected until they cause major problems. This appendix also presents various methods for managing detected failures by either working around them or correcting the erroneous condition. The methodologies presented include topics such as redundancy and diversity [15].

Part 3 focuses on the software requirements aspects, and steps through the software specific life cycle phases. These phases are software safety requirements specification, software safety validation planning, software design and development, programmable electronics (PE) integration, software operation and modification procedures, and software safety validation. The specific requirements for each of these phases are identified throughout section 7 of Part 3 [24].

The appendices of Part 3 provide lists of techniques and methods that can be selected to reach the desired safety integrity level. For each technique and method it is indicated as highly recommended, recommended, impartial, or not recommended for each safety integrity level. This information is presented in tabular format throughout appendices A, B, and C that provides a very useful tool for the planning phase of a project [24].

ISA 84.00.01(IEC 61511 Mod)

The International Society of Automation's standard on process safety has experienced an evolution over the years and the current version is mostly an adoption of the IEC 61511 standard. ISA 84.00.01 is a three part standard and is the process industry's specific implementation of IEC 61508 [32]. The common practice in the process industries is expected to be that manufacturers of safety instrumented system equipment will mainly utilize IEC 61508 while the process industry end users mainly utilize ISA 84.00.01 (IEC 61511 Mod). The bulk of the requirements are in Part 1 [16] of ISA 84.00.01 so this survey will focus on that section. Part 2 [33] covers guidelines for the application of Part 1, and Part 3 [10] provides guidance on the evaluation of risk in order to determine the appropriate safety integrity level to be specified. This evaluation includes a discussion of classification process for equipment in the process industry so it will be reviewed as well.

Part 1 of this standard covers framework, definitions, system, and hardware and software requirements for SIS. More specifically, it discusses management of functional safety, safety life-cycle requirements, verification, process hazard and risk assessment, allocation of safety functions to protection layers, SIS safety requirements specification, SIS design and engineering, requirements for application software, including selection criteria for utility software, factory acceptance testing, SIS installation and commissioning, SIS safety validation, SIS operation and maintenance, SIS modification, SIS decommissioning, and information and documentation requirements [16].

Because of the expected audience of this standard being end users and not manufacturers, the discussions are less detailed concerning individual components than the corresponding discussions in IEC 61508. Instead, the discussions are focused on the implementation of SIS's from a higher level, plant system perspective. A specific example of this is the topic of hazard and risk assessments. The end user has an advantage over the manufacturer in this area because the scope of potential applications of equipment can be reduced. This is because the end user knows how and where the equipment will be used and what the overall architecture of the system will be. A manufacturer intentionally keeps the scope of potential applications very broad so that they can sell their equipment to more customers [16].

In order to maintain harmony between IEC 61508 and ISA 84.00.01(IEC 61511 Mod) the overall framework of IEC 61508 is maintained in ISA 84.00.01. For example, the safety integrity level scheme (SIL 1, 2, 3, & 4) remains exactly the same. One interesting note from ISA 84.00.01 regarding SILs is that the application of SIL 4 criteria is considered very unusual in the process industry and it is recommended to attempt to redesign a system to reduce its safety significance to a lower SIL before embarking on an effort to implement a system at SIL 4. It is further noted that SIL 4 is considered to be very difficult to achieve and maintain.

Part 3 of ISA 84.00.01 describes the allowed methodologies for classifying equipment. These methodologies are similar in the manner of increasing requirements based on the importance of a specific safety system to the overall safety of the plant. Both qualitative and quantitative methods are allowed for determining the SIL that will be required for a particular safety system. The concept of SILs can be confusing as it is not considered an equipment classification system in that it is not categorizing equipment based on the risk that is associated with them. Instead, it is standardizing a level of rigor to be applied to establishing the evidence of equipment's design integrity. Figure 3.1 illustrates this concept.

The design requirements for SIS include built in features to defend against random and systematic failures. Some of these requirements involve system behavior on detection of a fault (e.g., includes the use of self-diagnostics) and hardware fault tolerance. The detection of faults is identified as potentially being performed by diagnostic testing, proof testing, or any other means. The required

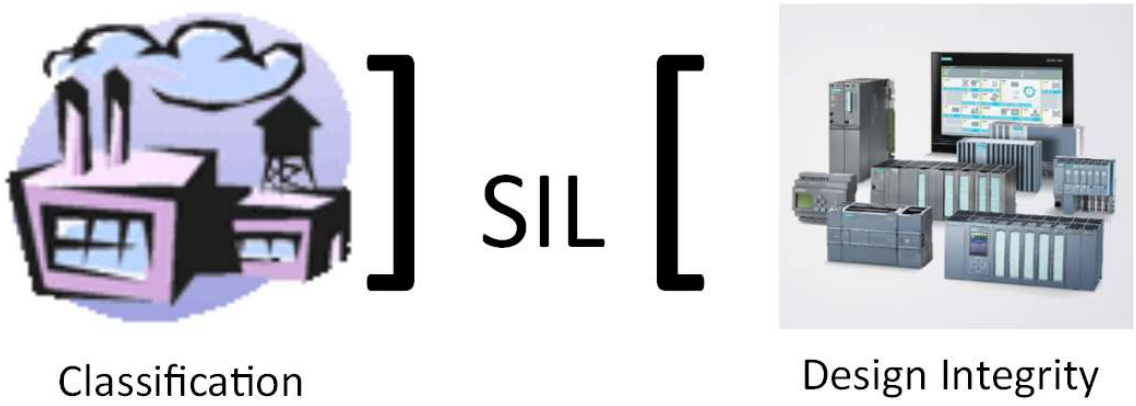


Figure 3.1. SIL Standardization
This is an illustration of the standardizing role SILs play between the classification of equipment at the plant and the design integrity established by the equipment manufacturer.

response to the detection of a fault varies based on the fault tolerance of the system. A response may range from a warning light illuminating to planned, systematic actions for the safe shutdown of the entire system. Hardware fault tolerance is defined as, “the ability of a component or subsystem to continue to be able to undertake the required safety instrumented function in the presence of one or more dangerous faults in hardware. A hardware fault tolerance of 1 means that there are, for example, two devices and the architecture is such that the dangerous failure of one of the two components or subsystems does not prevent the safety action from occurring.” [16]

In ISA 84.00.01, an assumption seems to be made within the SIS requirements section that alludes to the option of selecting off-the-shelf (OTS) or pre-existing equipment. There are discussions of components designed and manufactured using IEC 61508, but there are also discussions of justifying the use of components based on prior use. The scenario involving prior use is assumed to be for equipment that was not designed and manufactured using IEC 61508 [16].

Several factors are identified as being necessary evidence for the determination of suitability for components based on prior use. These factors are identified as follows: consideration of the manufacturer’s quality, management, and configuration management systems, adequate identification and specification of the components or subsystems, demonstration of the performance of the components or subsystems in similar operating profiles and physical environments, and the volume of the operating experience. These factors are considered as mitigating strategies for equipment not designed and

manufactured using IEC 61508, but it is understood that the higher the SIL that is needing to be achieved, the harder it is to achieve by using a prior use basis [16].

Additionally, on the topic of selection of components and subsystems for use within SISs, an aspect that appears to streamline their implementation for the process industry is that there are several components and subsystems that are certified as having been designed and manufactured to the requirements of IEC 61508 [39]. This results in having several suitable options available “off the shelf” or pre-existing. That is unique for most industries that use instrumentation and control equipment to mitigate significant risks.

The software requirements addressed in ISA 84.00.01 are limited to the application software that is developed using a fixed program language (FPL) or limited variability language (LVL) for up to SIL 3 SISs. This is consistent with the understanding of the target audience being process industry end users and not equipment manufacturers. Readers are referred to Part 3 of IEC 61508 for coverage of utility software (software development tools), embedded software (platform software supplied with the equipment from the manufacturer), and application software written using a full variability language (FVL) or is intended for use in a SIL 4 SIS [16].

Within this limited scope, the realization phase of the application software life cycle is described as consisting of the requirements specification, validation planning, design configuration and simulation, integration, and operation and modification procedures. For these specific topic areas, the content is consistent with corresponding sections of IEC 61508 Part 3, but emphasizes the role of the system integrator, end user, or plant design engineering group [16].

Commercial Nuclear Power Generation

General

Since the first nuclear power plant was connected to the commercial utility power grid in 1954 at Obninsk, USSR [40], the commercial nuclear power generation industry has been highly regulated. This is mostly due to it being inherently related to the most powerful weapon currently known to man, the nuclear bomb. The aspect of nuclear fission of being able to release very large amounts of energy both make it very beneficial and also make it potentially very harmful. Over time, heavy regulation was also supported by accidents experienced in commercial nuclear power plants such as the Three Mile Island, Chernobyl, and Fukushima [41]. These accidents demonstrated the potential harm involved in utilizing this technology.

Regulation is mainly a nation by nation activity but efforts have been made to move it up to an international level. In 1996, the Convention on Nuclear Safety (CNS) was formed by the International Atomic Energy Agency (IAEA). The CNS was focused on, “to legally commit participating States operating land-based nuclear power plants to maintain a high level of safety by setting international benchmarks to which States would subscribe” [42]. “The Convention is based on

Parties' common interest to achieve higher levels of safety which will be developed and promoted through regular meetings. The Convention obliges Parties to submit reports on the implementation of their obligations for 'peer review' at meetings of the Parties to be held at the IAEA." [42]. At this point in time, 78 nations have joined the CNS. Each individual nation remains independently responsible for establishing or endorsing the laws, rules, and standards that nuclear power plants must meet, but through the CNS, each nation is responsible to ensure that their regulatory program meets a universally accepted set of safety principles.

Because of the focus on the individual nations, this survey will be structured to review a select group of nation's programs implemented to ensure safety of nuclear instrumentation and control (I&C) systems. A group of applicable international standards will be reviewed initially independent of a particular nation, followed by a discussion to identify whether the international standards are utilized during the review of each nations' laws and standards.

International Standards Structure

The international standards organization applicable to the safety of nuclear I&C systems is the International Electrotechnical Commission (IEC). The IEC has a set of standards created by its subcommittee 45A of technical committee 45: Nuclear Instrumentation. The parent standard in this hierarchy of documents is IEC 61513 [22]. This document presents the broad collection of design aspects involved in nuclear I&C safety systems without going into detail, but instead presents a high level road map. There are several daughter standards that cover specific topics in the necessary detail (only a subset is described in this survey). See Figure 3.2 for more detail on the IEC hierarchy. IEC 61513 is also considered the nuclear power industry implementation of IEC 61508 [15], [24], [32], [35]–[38]; which has been previously described as a non-industry specific safety standard that was created by the IEC Subcommittee 65A of Technical Committee 65.

The methodology presented by IEC 61513 [22] is structured into a layered lifecycle approach. It is intended to link the nuclear power plant's (NPP) overall safety requirements to the safety requirements of the individual I&C systems. Figure 3 of the standard provides an interesting visual illustration of the aspects of systematic faults versus random failures. This standard lays the framework to address both types of concerns. The aspects of assessing reliability focus on defending against random failures, while the majority of life cycle phases focus on the elimination of systematic faults.

The top layer is the overall plant I&C safety. Phases included in this overall plant I&C safety life cycle are as follows: review of the plant safety design base, definition of the overall requirements specification, design of the overall I&C architecture and assignment of functions to individual systems and equipment, overall planning, realization of individual systems, overall system integration and commission, and overall operation and maintenance. The phase

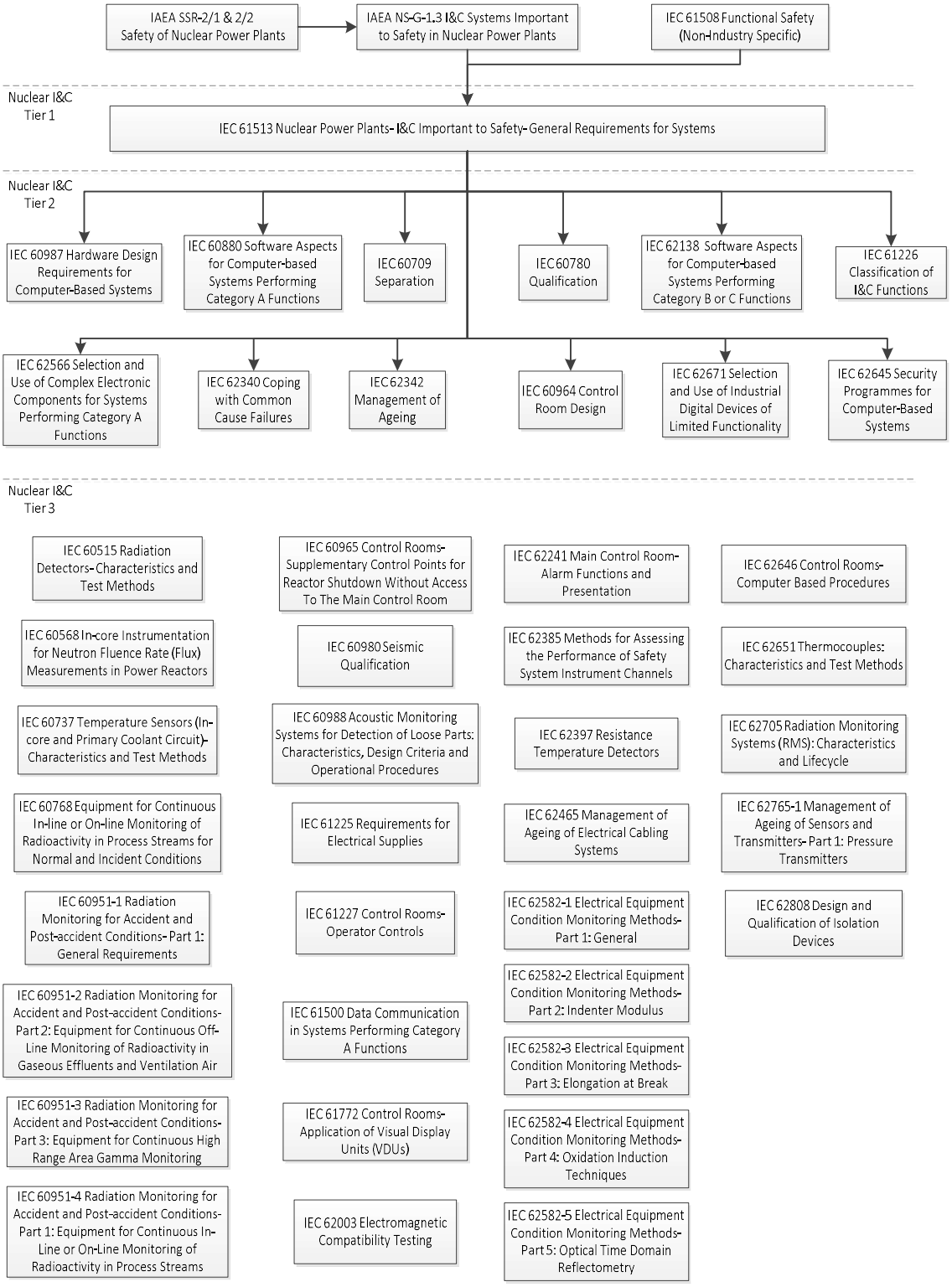


Figure 3.2. IEC Standards Hierarchy
The complete list of IEC nuclear I&C standards are shown sorted into their four tiered structure

of design of the overall I&C architecture is where the use of hazard analysis is incorporated to ensure the requirements are properly defined. The overall design phase is also where principles such as defense against common cause failure is incorporated. During the overall planning phase is where system security is addressed and planned for [22].

The lower layer is system safety life cycle. Phases include in this life cycle are system requirements specification, system specification, detailed design and implementation, integration, validation, installation, and modification. The system specification phases is where the treatment of pre-existing (i.e., COTS) equipment is addressed through the description of a suitability analysis. Several other safety principles are addresses within this life cycle layer such as independence of redundant channels, additional defense against CCF, and reliability assessments. For additional hardware requirements, IEC 60987 [23] is pointed to throughout this lifecycle layer. For requirements specific to software, IEC 60880 [25] and IEC 62138 [26] are referenced throughout this life cycle layer [22].

This standard also provides guidance concerning the quality assurance program that should be used by the entity designing and manufacturing the safety system or component. This guidance generally pointed to ISO and to IAEA GS-R-3 and IAEA GS-G-3.1 [22].

The first daughter standard that needs to be considered covers the topic of classification and lays the framework for implementing a graded approach to the design of I&C safety systems. This standard is IEC 61226 [13] and prescribes three function categories (A, B, and C), and three equipment classes (1, 2, and 3). Categorizing I&C functions is described as mainly being a deterministic process (supplemented with probabilistic techniques when appropriate), using descriptions of what types of safety functions fit into each category. These categories are laid out in a defense-in-depth format with Category C being the first layer of safety and Category A as being the final and most critical layer [13]. These categories are used by the rest of the standards in the series to identify the requirements that apply to the systems performing the functions that fall into each of the categories. The equipment classification is then set by the category of the function it will be performing. Namely, Class 1 equipment can perform category A, B, or C functions. Class 2 equipment is limited to performing category B and C functions. Class 3 equipment is further limited to only performing category C functions. This correlation between categories and classes is shown in Table 2 of IEC 61513 [22].

To address computer-system hardware requirements for class 1 and 2 equipment there is IEC 60987 [23]. Class 3 equipment does not have any additional requirements beyond what is considered typical for normal commercial grade. Topics covered in this standard are design, verification and validation, environmental qualification, manufacture, installation, maintenance, modification, operation, reliability/availability, and use of pre-existing hardware. Overall, this standard describes the specifying of functional, performance, reliability,

availability, environmental withstand, and documentation requirements following a top down approach where the equipment is designed to meet the requirements. One method identified for addressing reliability is the use of hazard analysis. Two specific methods mentioned are fault tree analysis (FTA) and failure mode and effect analysis (FMEA).

This standard also addresses the increasingly common situation where pre-existing equipment is utilized. These situations force more of a bottom up derivation of requirements. In order to utilize this pre-existing equipment, requirements must be carefully specified in a manner that allows the equipment to be acceptable while also maintaining all of the overall safety requirements of the nuclear power plant (NPP).

There are two standards that address software requirements for safety equipment. IEC 60880 [25] addresses equipment that will be used to perform category A functions (class 1). This standard describes the life cycle phases for the development, use, and modification of the software used in this class of equipment. It also addresses the qualification of pre-developed software (also known as commercial off the shelf), and includes what is described as a suitability analysis. Software design concepts that are covered include derivation of requirements, system security, incorporation of self-diagnostics, response to detected faults, use of modular source code, programming best practices, treatment of software development tools, and defense against common cause failure. Software verification topics described were desired characteristics of verification personnel, development and use of a plan, use of code inspections, use of analysis (potentially with automated tools), and use of tests.

IEC 62138 [26] addresses equipment that will perform category B (class 2) and/or category C (class 3) functions. Three different types of software systems are described; human machine interface (HMI), automation and control, and service systems. These types are described as also being able to be broken down into previously developed (typically system software) and new software (typically application software). For these types of equipment, a lifecycle approach is described that is less rigorous than what is described in IEC 60880 but still ensures adequate assurance of safety is maintained. As such, the methodologies described in this standard are molded to be more explicitly achievable for pre-existing systems.

The topic of environmental qualification, the process of verifying that equipment will withstand the environmental conditions they will be exposed to in their application within the nuclear plant, are addressed by a collection of standards with the overall standard being IEC 60780 [43]. There are several lower-tiered standards used to cover the various aspect of this topic. Two examples are IEC 60980 [44] for addressing resistance to seismic events and IEC 62003 [45] to address electromagnetic compatibility.

The final daughter standard to be discussed is IEC 62645 [46]. This standard covers the requirements to be met for security programs of computer based systems used in nuclear power plants. This standard establishes three

levels of security classifications. These levels are completely different from the safety classifications described in IEC 61226; they are referred to as security degrees instead of security classifications and are identified as S1, S2, and S3. The standard includes a description of a life cycle process and identifies how security must be worked into all phases, including design, operation, and retirement.

United States of America

The first specific country's laws, regulatory framework, consensus standards, and industry guidance to be surveyed is the United States of America. The original legislation related to nuclear power was the Atomic Energy Act of 1954. This Act created the Atomic Energy Commission and resulted in provided general principles and concepts but left the regulation enforcement open ended. This was later addressed by the Energy Reorganization Act of 1974. This Act dissolved the Atomic Energy Commission and established the Nuclear Regulatory Commission (NRC). The NRC has been the regulating body of commercial nuclear power ever since [47].

To regulate the licensing of commercial nuclear reactors the NRC has established two laws. The first was Title 10 Code of Federal Regulations (CFR) Part 50 [48] (10 CFR Part 50). This licensing approach involved two parts: a construction permit and an operating license, and is assumed to have been originally established in the late 1970s. All currently operating US commercial nuclear reactors used this methodology [47].

The second law was 10 CFR Part 52 [49] and was established in 1989. This approach allows for the use of certified designs and combined construction and operation licenses [47] . Most of the new US plants currently under construction are using this approach because it is thought to reduce risk of not being able to obtain the operating license after construction is completed [50].

10 CFR Part 50, Appendix B [51] provides the requirements for the quality assurance programs that must be implemented at nuclear facilities and at vendor facilities who are supplying parts, systems, and services to the nuclear plants. One method established to meet the requirements of this law is the industry consensus standard ASME NQA-1 [52] which provides additional details for the implementation of a nuclear quality assurance program.

10 CFR Part 21 [53] establishes requirements for the reporting of defects and noncompliance. These requirements are typically applicable to all US nuclear power plants and any vendor that is interacting with parts and/or systems that are classified as safety related within their nuclear power plant application. To specifically address the requirements of safety systems, the NRC issued Regulatory Guide 1.152 (currently at Revision 3) [54] to endorse the Institute of Electrical and Electronic Engineers (IEEE) standard 603 [11]. This standard addresses a similar scope as IEC 61513 [22] by addressing safety system design requirements at an overall high level, but at this point in time, the NRC does not endorse the IEC standard. This is partly because there is significant history in the

relationship between the NRC and the IEEE. See Figure 3.3 for more detail about the IEEE standards. IEEE 603 originally existed long before IAEA NS-G-1.3 or IEC 61513 and the IEEE standards are the primary consensus documents used by the NRC. Regulatory Guide 1.152 Revision 3 goes on to also endorse IEEE 7-4.3.2 [17] to specifically address safety systems that involve the use of computers. IEEE 7-4.3.2 covers, at a high level, a similar scope as IEC 60987, IEC 60880, and IEC 62138, but once again the NRC does not currently endorse any of those IEC standards at this point in time.

IEEE 603 is not explicitly specific to instrumentation and controls as it covers the power systems as well. This standard presents safety system criteria that influences the safety system through all or certain phases of its life cycle, but the standard does not prescribe a specific life cycle format to be followed [11].

This standard addresses classification of equipment in a very deterministic and simple manner. Classification is made up of two categories: Class 1E and Non-class 1E. The definition of Class 1E is “The safety classification of the electric equipment and systems that are essential to emergency reactor shutdown, containment isolation, reactor core cooling, and containment and reactor heat removal, or are otherwise essential in preventing significant release of radioactive material to the environment.” The Class 1E classification considers equipment involved in performing any of the functions listed above. If it is not involved in performing any of those functions then it is Non-class 1E [11].

A safety system is described as being able to be divided into three components: sense and command, execute, and power sources. The standard first addresses general safety system criteria that is applicable to all three safety system components. One of the principles defined is the single-failure criterion. This is the concept that no one failure should be able to cause the safety system to fail overall to perform its Class 1E function. Analysis of the single failure criterion is intended to be deterministic, but an allowance is made for the use of a probabilistic assessment to eliminate any events or failures that are not credible (realistically impossible). Another principle is quality. This concept is focused on achieving minimal maintenance and low random hardware failure rates. The standard points to ASME NQA-1 [52] for guidance on the use of a quality assurance program, and points to IEEE 7-4.3.2 [17] for systems using digital technology. The next principle to note is equipment qualification. This concept is that safety system equipment shall be capable of functioning properly within the environmental conditions it will encounter when installed within the nuclear power plant. The standard points to IEEE 323 [55] for additional requirements related to this principle. Then there is the principle of independence. This refers to the requirement of independence between redundant portions of a safety system and independence between safety systems and other systems. This principle is important because, if proper independence is not maintained, the safety system’s resistance to single failures preventing the safety function may be lower than what is established in the safety system analyses. Another principle is reliability. Qualitative or quantitative reliability goals set for the safety system must be ensured to be met. A proven method for assessing system

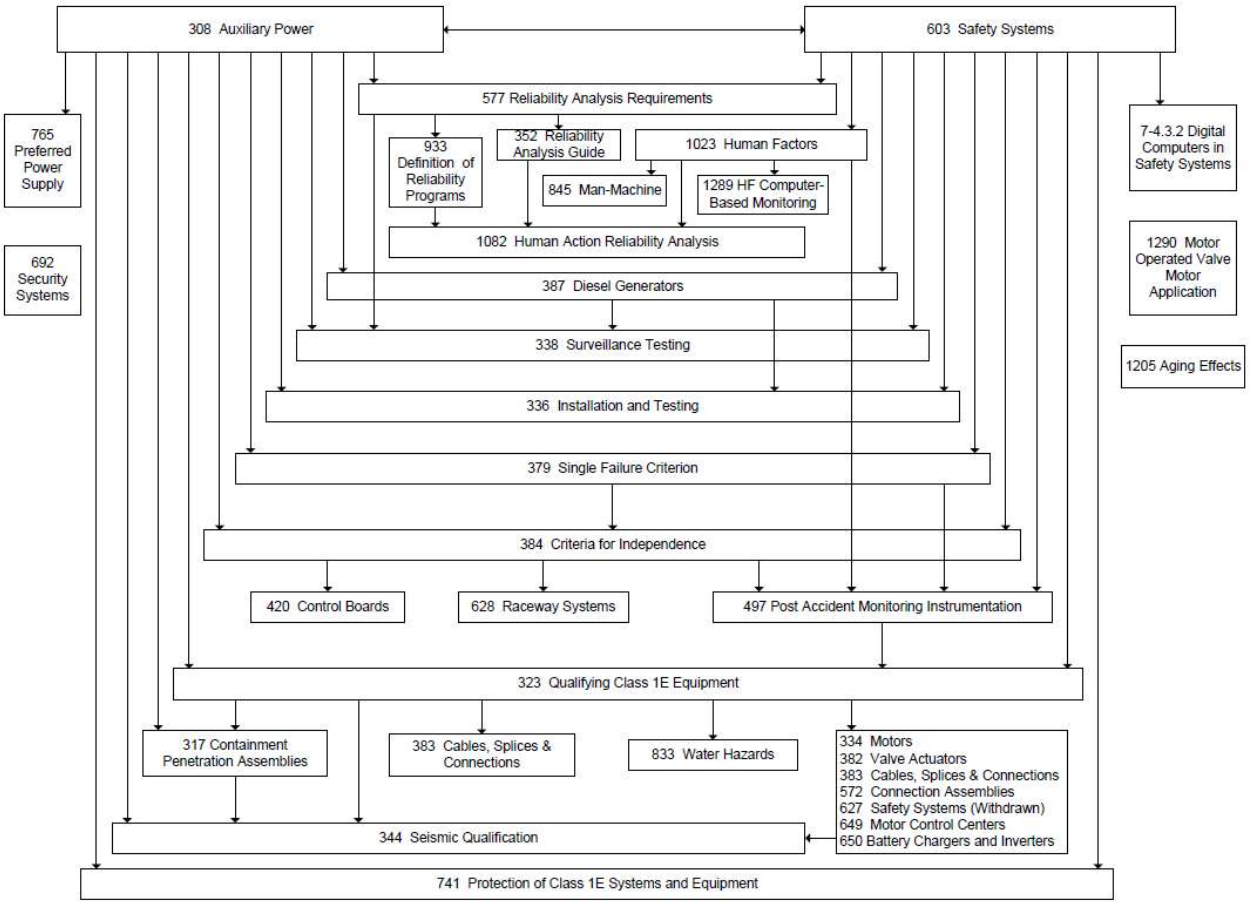


Figure 3.3. IEEE NPEC Standards [56]
The IEEE Nuclear Power Engineering Committee standards are show with relational links that identify the hierarchical structure

reliability must be implemented and IEEE 7-4.3.2 is pointed to for determining reliability of a system that involves computers. The last principle to be discussed is common-cause failure. This concept provides criteria for protecting the safety system from failing due to simultaneous systematic faults in multiple redundant portions of the system [11].

One issue that this standard does not address is how pre-existing (i.e., COTS) equipment should be assessed for suitability to be used in the safety system. Another issue to note as being not addressed is that, beyond the discussion of control of access, security is not discussed.

IEEE 7-4.3.2 [17] is set up to amplify the requirements of IEEE 603 [11] in the areas that require additional information to address the use of computers in the safety system. The principle of quality introduces the safety system life cycle concept and includes phases of establishing of system requirements, development of a detailed design, implementing the design, validating that the system performs as required, installation and site acceptance testing, operating and maintaining the system, and retiring the system. This principle of quality also leads to the issues of software development, use of pre-existing computers, use of software tools, verification and validation, configuration management, and risk management. Another principle that is enhanced is equipment qualification. An explicit note is added to ensure all portions of the system needed for performing the safety function are active during qualification by test. The principle of independence is expanded extensively to address the many potential interfaces computer systems could have. These expansions include buffering function/circuit, communication, and data. The issue of security is also extensively expanded within the principle of control of access. This section goes beyond physical security to get into virus protection, security patches, and the implementation of secure development environments into the safety system life cycle. Concerning the principle of reliability, the issue of software errors is identified as being best dealt with recording and trending their occurrences and combining that data with analysis, field experience, and/or testing. The next principle to be expanded on is common cause failure. This expansion is extensive because this principle is viewed as most impacted by the incorporation of computers into safety systems [47]. An analysis that can be used concerning common cause failure is a defense in depth (D3) analysis. The addition of diversity to the redundant portions of the safety system is identified as an ideal way to protect against common cause failures, but detailed analysis of the specific equipment to be used is prescribed to ensure there is not a common thread in the design development that could result in a common cause failure in equipment that appears to be diverse. The final principle that is addressed is the determination of suitability of use of digital COTS equipment. The use of commercial equipment for performing Class 1E functions involves a process called commercial grade dedication and is best described in an industry guidance document developed by the Electric Power Research Institute (EPRI). This document is EPRI 3002002982 [27] and is often referred to as Revision 1 of

EPRI NP-5652. A suitability analysis is described that involves performing an extensive design review (referred to as a critical digital review). The design review involves evaluating the commercial life cycle process used by the manufacturer to design and manufacture the equipment. It also involves a hazard analysis to study the behavior of the commercial equipment against its interfaces to the rest of the safety system. For additional details on performing the suitability evaluation (i.e., commercial grade dedication) this standard refers to some other industry guidance documents: EPRI TR-106439 [28] and EPRI 1011710 [29]

As previously mentioned, IEEE 323 [55] addresses equipment qualification from a high level. It is aided by several other standards to define the many nuances of this topic. One such standard is IEEE 344 [57] to address determining an equipment design to be adequately rugged to handle a credible earthquake at the nuclear power plant.

France

The second country to be surveyed is France. The first action the French government took regarding nuclear energy was in 1945 when they created the French Atomic Energy Commission. This entity was later renamed the French Alternative Energies and Atomic Energy Commission (CEA) in 2010. All commercial nuclear reactors in France have been and continue to be built and operated by the licensee Électricité de France (EDF). The French nuclear safety authority (ASN) was created by the Nuclear Security and Transparency (TSN) Act in 2006 in order to better promote transparency and security. The ASN is tasked with “monitoring nuclear safety and radiation protection, to protect workers, patients, the general public and the environment against the risks associated with civil nuclear activities” [58]. The ASN’s focus currently is to create basic nuclear installations (BNIs) to promote and explain the ASN doctrine. The effort to create BNIs was initiated by the “BNI procedure” decree of 2007 and is focused on the creation of “a rigorous, comprehensive working framework” [58] . The intent is for this framework to be harmonized with the other European nations utilizing nuclear power. This harmonization is being driven by the Western European Nuclear Regulators’ Association (WENRA). A goal of this effort is to assure that, “The requirements concerning the safety case to be provided by the licensee are broadly based on the IAEA standards” [58]. Drafting these safety requirements is the responsibility of the AFCEN (French association for rules on design, construction and in-service monitoring of nuclear steam supply systems). This group, made up of EDF and Areva NP, is responsible for directing compliance with the ASN’s BNIs through the creation of design and construction rule (RCC) codes. In order to maintain the trend of harmonization with other nuclear powered European nations and the standards of the IAEA, these requirements are being drafted to follow the methodologies laid out by IEC 61513 its numerous daughter IEC standards [59], some of which have been previously discussed in an earlier section of this survey.

Due to the recent creation of the French regulatory framework and currently ongoing activities to improve transparency, the specific design methodologies implemented in the existing nuclear power plants regarding the I&C safety systems is not clear. It appears reasonable to assume that future nuclear power plants will implement the design requirements and methodologies prescribed in the IEC nuclear I&C collection of standards.

United Kingdom

The United Kingdom's primary legislative framework for the regulation of the commercial nuclear power industry is made up of the Health and Safety at Work etc. Act of 1974, the Nuclear Installations Act of 1965 (as amended), the Radioactive Substances Act of 1993 (RSA93), Environmental Permitting (England and Wales) Regulations 2010, Energy Act of 2004, and the Freedom of Information Act of 2000. The Health and Safety at Work etc. Act of 1974 created the statutory body of the Health and Safety Executive (HSE). The Office for Nuclear Regulation (ONR) was originally formed in 2012 as a non-statutory Agency of the HSE. The ONR's responsibilities encompass those of the previous Nuclear Directorate and the Department for Transport's Radioactive Materials Transport Team of the HSE [60]. On the 18th of December 2013, the Energy Act was passed and the ONR was placed "on a statutory footing" [61]. The UK is also participates in WENRA and is interested in harmonizing its regulatory frame work with the other participating nations and the IAEA standards [60].

The desire for harmonization has driven the methodology used in the UK for implementing safety systems to the same IEC standards that France and much of Europe are moving towards. Thorough the WENRA and in partnership with Belgium, Germany, Spain, Sweden, and Finland a common position has been issued that describes the methodologies deemed appropriate for designing and implementing safety systems (including systems utilizing software). Included in these common positions are the topics of system classes, function categories, pre-existing software, tools, security, diversity, and a life cycle approach that includes specifications, design, implementation, verification, and validation [62].

Regarding system classes and function categories, a deterministic approach is utilized. A simplified implementation of the IEC 61226 [13] methodology is embraced. Category A as defined by IEC 61226 is implemented as safety systems. Categories B and C (according to IEC 61226) are implemented as safety related systems. Then equipment performing functions that do not fit in any of the IEC 61226 categories is considered as systems not important to safety [62].

For the topic of pre-existing software (PSW), the common view point is shared that not only is the use of such components beneficial for efficiency but may also increase confidence in safety [62]. This common position is heavily based on IEC 61513, IEC 60880, and IEC 60987 as previously discussed.

To be able to accept PSW, several aspects are needed to be verified. First, it needs to be verified that the PSW provides all the proper functionality that

will be required by the host safety system. Second, the extra features contained by the PSW cannot prevent the PSW from performing its critical functions depended on by the host safety system. Third, if some of the functions of the PSW are omitted the host safety system needs to still be able to perform its safety function. Fourth, the PSW and its associated development life cycle documentation need to be compared to the applicable standards to analysis for compliance. Fifth and finally, the critical functions of the PSW depended on by the host safety system need to be validated by testing.

Furthermore regarding PSW, properly documented and relevant operational experience can be credited to support claims of dependability. Operational experience is viewed as being complementary evidence support existing evidence from verification and validation activities that were performed on the PSW [62].

Concerning the use of software tools, the methodology implemented aligns well with IEC 60880. Software tools that have the potential of inserting errors into the software product must be validated before they can be accepted for use in designing that software product. Approaches to validating tools are inspecting the output of the tool for correctness with every use, or certification of the tool as being correct [62].

For the topic of security, the requirements align with IEC 61513 and IEC 60880 (IEC 62645 did not yet exist when the material being reviewed was prepared). The scope of the requirements range from physical security to the prevention of access to hackers, and also to the periodic auditing of system parameters to prevent an insider threat [62].

Regarding diversity, it is seen as a valuable defense against common cause failure. While redundancy, by itself, is protection against random hardware failures, to add diversity between those redundant channels builds in protection against systematic common cause failures. The concept of independence is an aspect of diversity. Complete independence between redundant portions of a safety system would cover a vast scope from the conceptual design, programming language, and software tools to aspects such as physical separation and isolated power sources. While it is not required to achieve complete independence, an effort must be made to achieve a reasonable level of independence and needs to be also coupled with the concept of defense in depth. The many aspects of diversity include the following: “functional diversity, technology diversity, independent teams for specifying, decomposing and deriving requirements, independent development teams with no direct communication, independent teams for performing verification and validation, different allocation of requirements to software components, different allocation of software components to hardware components, different timing and different order of execution, simplicity of software design and implementation, different description/programming languages and notations, different development methods, different development platforms, tools and compilers, different

operating systems, different hardware, diverse verification and validation" [62]. This overall concept aligns with IEC 61513 and IEC 60880.

For the topic of a life cycle approach to specifying, designing, implementing, verifying, validating, and then operating safety systems, the methodology embraces the concepts of IEC 61513. It is important to focus on the steps of specifying the system requirements before jumping into the implementation phase. The common tendency of technical personnel is to jump into building something but in order to end up with the best end product possible it is important to be disciplined and identify the requirements and plan out the design. This approach makes it much easier for the design work to be checked and/or audited later [62].

United States Department of Defense

The US Department of Defense (DOD) encompasses the Army, Navy, and Air Force has roots that go back to 1775 and the American Revolution. The DOD's literature provides this description of its history:

> *The Army, Navy, and Marine Corps were established in 1775, in concurrence with the American Revolution. The War Department was established in 1789, and was the precursor to what is now the Department of Defense.*
>
> *One year later, in 1790, the Coast Guard (part of Homeland Security in peace time) was established. This was followed by the founding of the Department of the Navy in 1798.*
>
> *The decision to unify the different services under one Department led to the creation of the National Military Establishment in 1947. This establishment would replace the War Department, which converted to the Department of the Army. That same year, the U.S. Air Force was established followed by the founding of the Department of the Air Force.*
>
> *Finally, the three military branches, Army, Navy, and Air Force, were placed under the direct control of the new Secretary of Defense, confirmed by Senate.*
>
> *In 1949, an amendment to the National Security Act further consolidated the national defense structure by withdrawing cabinet-level status from the three Service secretaries. The National Military Establishment was then renamed the Department of Defense* [63].

The DOD covers a large scope of applications for safety systems and mission critical computer applications, and puts extensive effort into the development those systems in a manner that allows them to have a very high level of correctness, reliability, and security. To this end, the DOD has issued several documents on this topic of safety systems and the main documents will be surveyed in this section.

MIL-STD-882E Standard Practice of System Safety

This document starts out by defining the main goal as being to eliminate hazards when possible and to minimize risks when hazards cannot be eliminated. The process for achieving this goal involves 8 elements. Those elements are: document the system safety approach, identify and document hazards, assess and document risk, identify and document risk mitigation measures, reduce risk, verify validate and document risk reduction, accept risk and document, and manage life-cycle risk[14].

During the assessing and documenting risks process, risks are categorized by severity and probability (frequency of occurrence). The probability levels are open to being defined as either qualitative or quantitative. Additionally it is acknowledged that software risks must be assessed differently. Due to inherent differences between the ways that hardware and software fail, predicting the probability of failure of software is very difficult and cannot be based on historical data. Instead software risks are assessed using software control categories along with the severity categories to determine a software criticality index (SwCI). The SwCI is then correlated into a level of rigor (LOR) that can be used to define what the safety requirements are for the software [14].

Concerning classification of equipment, some specific terms are described in this standard. Those terms are safety-related, safety-critical, and safety-significant. Safety-related is “a term applied to a condition, event, operation, process, or item whose mishap severity consequence is either Marginal or Negligible”. Safety-critical is “a term applied to a condition, event, operation, process, or item whose mishap severity consequence is either Catastrophic or Critical”. Safety-significant is “a term applied to a condition, event, operation, process, or item that is identified as either safety-critical or safety-related”. Even though these terms have been defined, their specific meaning will vary based on the nature of each specific project.

Hazard analysis is a significant aspect of the methodology prescribed in this standard. The sequence of hazard analyses is the Preliminary Hazard Analysis (PHA), System Requirements Hazard Analysis (SRHA), Subsystem Hazard Analysis (SSHA), System Hazard Analysis (SHA), Operating and Support Hazard Analysis (O&SHA), Health Hazard Analysis (HHA), Functional Hazard Analysis (FHA), System-of-Systems (SoS) Hazard Analysis, and Environmental Hazard Analysis (EHA) [14].

In summary, this standard does not prescribe the use of any specific design architectures or methodologies to achieve safety. Instead, it is focused on the elimination and management of the risks involved and drives documentation of the specific methodologies that are implemented. It also prescribes the verification steps to ensure the implementations comply with the safety requirements that were derived from the hazard analyses [14].

Joint Software Systems Safety Engineering Handbook

This handbook is written in a manner to address implementation of software system safety (SSS) as a subset within the overall concepts of system safety engineering. The implementation of a systems perspective to maintaining safety means that a complete view of the components, interfaces, and impacting factors is maintained to ensure comprehensive solutions are identified and implemented. This approach is in contrast to a methodology that would focus in on specific aspects of the system and attempt to design and implement those specific components without fully understanding how all the system will ultimately end up working together. System safety program requirements are identified as including:

- Eliminate identified hazards or reduce associated risk through design, including material selection or substitution
- Isolate hazardous substances, components, and operations from other activities, areas, personnel, and incompatible materials
- Locate equipment so that access during operations, servicing, maintenance, repair, or adjustment minimizes personnel exposure to hazards
- Minimize risk resulting from excessive environmental conditions (e.g., temperature, pressure, noise, toxicity, acceleration, and vibration)
- Design to minimize risk created by human error in the operation and support of the system
- Consider alternate approaches to minimize risk from hazards that cannot be eliminated. Such approaches include interlocks; redundancy; fail-safe design; fire suppression; and protective clothing, equipment, devices, and procedures
- Protect power sources, controls, and critical components of redundant subsystems by separation or shielding
- Ensure personnel and equipment protection (when alternate design approaches cannot eliminate the hazard) provide warning and caution notes in assembly, operations, maintenance, and repair instructions as well as distinctive markings on hazardous components and materials, equipment, and facilities. These shall be standardized in accordance with MA (Managing Authority) requirements
- Minimize severity of personnel injury or damage to equipment in the event of a mishap
- Design software-controlled or monitored functions to minimize initiation of hazardous events or mishaps [1]

On the path to eliminating and reducing risk as much as possible, there are some general methodologies laid out in an order of precedence. Those are:

- Design for Minimum Risk – From the first, design to eliminate hazards. If an identified hazard cannot be eliminated, reduce the

associated risk to an acceptable level, as defined by the MA, through design selection.

- Incorporate Safety Devices – If identified hazards cannot be eliminated or their associated risk adequately reduced through design selection, that risk shall be reduced to a level acceptable to the MA through the use of fixed, automatic, or other protective safety design features or devices. Provisions shall be made for periodic functional checks of safety devices when applicable.
- Provide Warning Devices – When neither design nor safety devices can effectively eliminate identified hazards or adequately reduce associated risk, devices shall be used to detect the condition and produce an adequate warning signal to alert personnel of the hazard. Warning signals and their application shall be designed to minimize the probability of incorrect personnel reaction to the signals and shall be standardized within like types of systems.
- Develop Procedures and Training – Where it is impractical to eliminate hazards through design selection or adequately reduce the associated risk with safety and warning devices, procedures and training shall be used. However, without a specific waiver from the MA, no warning, caution, or other form of written advisory shall be used as the only risk reduction method for Category I or II Mishaps. Procedures may include the use of personal protective equipment. Precautionary notations shall be standardized as specified by the MA. Tasks and activities judged to be safety-critical by the MA may require certification of personnel proficiency [1].

This handbook intends to address the aspects and roles that software plays within the overall system concept. It is also important to note that the systems perspective includes the implementation of a life cycle approach to the specification, design, implementation, verification, and operation processes. Another note on this handbook is that it approach to assessing and defining risk is consistent with MIL-STD-882E [14]. It includes the same severity categories, probability levels, software control categories, and software criticality index [1].

Another aspect of this handbook that is consistent with MIL-STD-882E [14] is the use of LORs (levels of rigor). After the software criticality index (SCI) is defined, it is correlated to a LOR and each LOR has a defined set of requirements that are then applied to that system software. Defining specific requirements for the LORs is a project specific activity, but they typically cover the scope of design requirements, process tasks, and test tasks. Some examples of design requirements are fault tolerant design, fault detection, redundancy, independence, and full COTS features disclosure and analysis. Some examples of process tasks are design reviews, code walkthroughs, independent reviews, and specific software language requirements. Some examples of test tasks are safety-significant function testing, 100% regression testing, verification and validation, and full screening of all COTS features [1].

This handbook describes the software safety task implementation steps that should be viewed as a baseline, understanding that there are specific cases that will require variations to this model. The defined steps are analyze conceptual design baseline, define software assurance LOR, functional hazard analysis, preliminary hazard analysis, safety requirements analysis, preliminary software design SSHA, detailed software design SSHA, and system hazard analysis [1].

The software design SSHA section of this handbook goes into some detailed descriptions of design and analysis techniques. While it does not identify any as requirements, it does provide useful information for assisting in identifying when certain techniques should be used and when they should not. Some of the techniques described are safety interlocks, come-from programming, control flow analysis, interrupt analysis, and formal proofs of correctness [1].

Appendix D of this handbook is specifically focused on use of commercial off the shelf (COTS) and non-developmental item (NDI) software. This appendix recognizes that, “The safety assessment of COTS and NDI software poses one of the greatest challenges to the safety assessment”. It also recognizes the advantages for utilizing this type of product as being, “cost savings (no development costs), rapid insertion of new technology, proven product/process, possible broad user base, potential technical support, and potential logistics support”. Unfortunately there are also significant disadvantages, as mentioned in chapter one of this thesis. Some of those are as follows: potential for limited development, test, or configuration control documentation, unknown development history, unavailability of design and test data, limited or no supportability from the developer or vendors, unavailability of safety analyses for the COTS application, or potential for increased test and analysis required for safety verification. The actual list of advantages and disadvantages may vary drastically from one specific situation to another but these are good points to consider when evaluating a decision to use this type of equipment [1].

The approach presented in this handbook for evaluating a COTS item for selection and use in a safety system is the confidence, influence, and complexity criteria. The confidence aspect is focused on achieving strong evidence that indicates the COTS item will successfully perform its critical functions when installed within the full range of possible operating environmental parameters. The influence aspect focuses on understanding the safety significance of the role of the COTS item within the host safety system. Finally, the complexity aspect focuses on a combination of safety factors, testability factors, and integration factors. With these three criteria (confidence, influence, and complexity) evaluations can be performed to make decisions about whether or not certain COTS items should be used within a particular safety system [1].

Appendix E of this handbook covers generic software safety requirements and guidelines. The high level topics covered include design and development process requirements and guidelines, system design requirements and guidelines, power-up system initialization requirements, computing system

environment requirements and guidelines, self-check design requirements and guidelines, safety-critical computing system functions protection requirements and guidelines, interface design requirements, human interface, critical timing and interrupt functions, software design and development requirements and guidelines, software maintenance requirements and guidelines, and software analysis and testing. While the information in this section is very detailed, it still allows for flexibility in the implementation of individual projects. This appendix can serve as a general checklist to assist in the completeness of the planning and executing of a specific project.

General Observations

The Department of Defense's approach to safety systems is geared very much towards process and intentionally does not focus on requiring specific design criteria. This makes sense when considering the wide range of systems that the DOD utilizes. Focusing on requiring specific design principles may unnecessarily limit certain design activities. Instead, the focus is on the identification of the risks involved in each specific project and defining the appropriate levels of rigor to be implemented to eliminate or reduce those risks appropriately. For some industries this approach of addressing each project individually would not be viable but, because the DOD will most likely purchase large quantities of each of these systems, it is.

CHAPTER FOUR

COMPARE AND CONTRAST METHODOLOGIES

Classification of Systems and Components

The use of classification methodologies for safety systems is all about ensuring a consistent level of rigor is applied to situations/applications in order to mitigate specific levels of risk. So a comparison of classification methodologies across different industries is also a comparison of the level of rigor (LOR) applied to those systems and components [14]. The main advantage to understanding the classification methodologies and understanding how they are the same is so that equipment used in a certain class of applications in one industry could also be used in an equivalent class of application in a different industry.

Overall, there is a theme through the various industries that the more important the system is to maintaining safety (often referred to as the safety significance) the higher the LOR is required to be. Underneath that theme there are factors such as likelihood of a hazardous event occurring and consequences of the hazardous event that are often considered to conclude how important a particular system is [12]. Within this overall theme the particular methodologies for determining which systems are most important to safety is where significant variability is observed.

Probabilistic vs Deterministic

Classification methodologies can be probabilistic, deterministic, or a combination of both. Probabilistic methodologies are those approaches that account for the expected likelihood of hazardous events occurring and their associated consequences, also described as risk. Deterministic approaches are those that don't account for probabilistic factors. Instead, they classify equipment based on factors such as specific functions the equipment will perform, and severity of the consequences of the equipment's failure [12]. Both deterministic and probabilistic methodologies can be described further as either being qualitative or quantitative. Quantitative approaches involve numerical values that can be calculated. A numerical indicator is calculated to represent key characteristics of the system being classified [36]. Qualitative approaches do not involve the use of any mathematical calculations and rely on factors that cannot be accounted for numerically [36].

All instances of the nuclear industry that were surveyed use a primarily deterministic and qualitative approach. The US nuclear industry (IEEE standards based) employs a simple two category strategy. Equipment is either Class 1E (safety) or Non-Class 1E (non-safety) and is put into these categories solely based on whether or not it is involved in a particular list of functions being performed in the plant [11]. The international nuclear industry uses a more expanded scheme but still deterministic and qualitative approach involving Categories A, B, C, and unclassified that is still based on a specific list of

functions. The key that makes these approaches deterministic is that there is a set relationship between the plant functions and the classifications without accounting for variability related to probability of failure. Both the international and US industries acknowledge that there is value in using methodologies that incorporate accounting of risk but those are currently viewed as no more than supplemental to the main deterministic approaches. The international industry does include an explicit direction for the deterministic approach to be complimented by probabilistic approaches when it is considered appropriate [12]. Another note on the international nuclear industry is that it classifies functions separately from actual equipment [13]. Once the functions are categorized, the equipment is classified as 1, 2, or 3 based on what functions that equipment will be performing [22].

<table>
<tr><th>National or international standard</th><th colspan="4">Classification of the importance to safety</th></tr>
<tr><td rowspan="2">IAEA NS-R-1</td><td colspan="3">Systems Important to Safety</td><td rowspan="2">Systems Not Important to Safety</td></tr>
<tr><td colspan="2">Safety</td><td>Safety Related</td></tr>
<tr><td rowspan="2">IEC 61226 Functions Systems</td><td colspan="3">Systems Important to Safety</td><td rowspan="2">Unclassified</td></tr>
<tr><td>Cat. A
Class 1</td><td>Cat. B
Class 2</td><td>Category C
Class 3</td></tr>
<tr><td rowspan="2">USA and IEEE</td><td colspan="3">Systems Important to Safety</td><td rowspan="2">Non-nuclear Safety</td></tr>
<tr><td>Safety Related, Safety, or Class 1E</td><td colspan="2">(No name assigned)</td></tr>
</table>

Figure 4.1. A Comparison of Different Classification Systems
The columns of this figure qualitatively illustrate the relationships between the different nuclear classification schemes and is extracted from Table 1 of Ref [64]

The US Department of Defense's approach to classifying equipment is considered probabilistic. Understanding and accounting for risk is a foundational aspect of the DOD's methodology. Their methodologies can mostly be described as qualitative more than quantitative but both are used. Concerning hardware and non-computer based systems, risk is evaluated using two factors: severity and frequency. For computer-based systems, risk is evaluated differently. Instead of frequency, a set of software control categories (SCC) are used that describe software characteristics from a high perspective and are assigned levels based on those characteristics' sensitivity to the prevention of hazards. To complete the evaluation of risk and the classification process, the SCC is then combined with the severity level of negligible, marginal, critical, or catastrophic. The combined result is the software criticality index and that is directly used to define the LOR to be applied. The software criticality index can range from 5

(calls for a low LOR) to 1 (calls for a very high LOR). Figure 4.2 illustrates this methodology.

When classifying safety systems, process industries use a probabilistic approach that starts by evaluating the risks and the necessary risk reduction, this is similar to the methodology of the US DOD. Another similarity between the DOD and the process industry is that there are a vast array of applications that must be able to be covered by the standards and methodologies. Once the risk is understood, the necessary risk reduction factors are specified. These risk reduction factors can be non-safety instrumented system prevention/ mitigation protection layers, SIS, and/ or other protection layers. Focusing on the use of SIS, the process industry allows for all possible qualitative and quantitative methodologies for determining what the safety integrity level (SIL) of the SIS needs to be [10]. One of those methodologies is a hazardous event severity matrix that is very similar to what is used by the DOD. The process industry does not specify exactly what factor is used on the vertical axis so an example is shown in Figure 4.3 of the number of risk reduction approaches that are being implemented in parallel. This is in contrast to the use of software criticality categories in Figure 4.2.

Level of Rigor

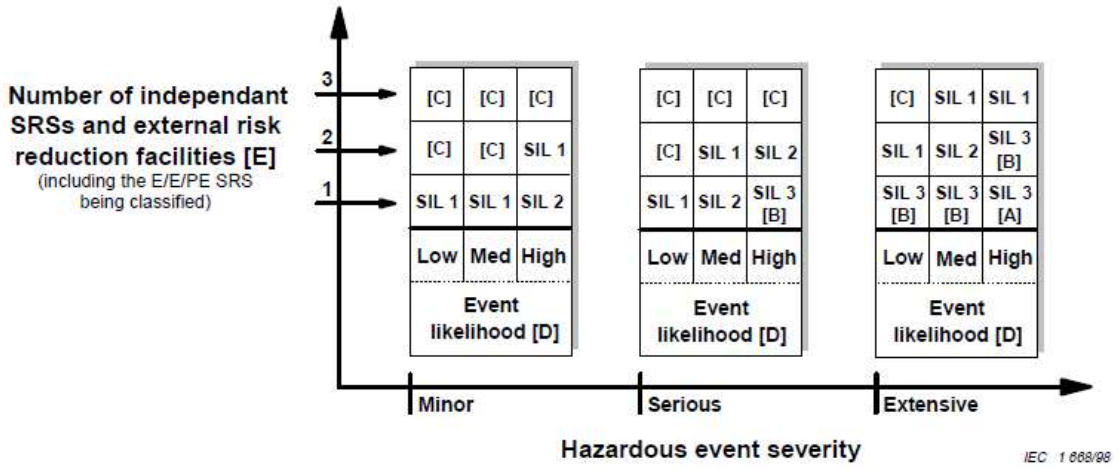
The actual design criteria and techniques used during the design and manufacturing process establish the level of rigor. Another way to think about it is that it is the driver for the building of the required level of evidence that the equipment will perform its function at the required level of reliability and safety integrity. The classification process sets the goals and the level of rigor meets the goals and provides the evidence to prove it.

One common perspective among the industries surveyed is that potential systematic faults (mainly from software-based systems) cannot be measured quantitatively the way potential random hardware failures of non-computer-based systems can. The involvement of software limits the effectiveness of the quantitative analysis techniques because software is not actually considered to ever fail. If the system is caused to behave in an undesirable manner because of the software, it is commonly viewed as a design fault. It is much more difficult to model errors in the software quantitatively the way a mechanical component can be predicted to fail through the use of a quantitative probabilistic model [1], [25], [32].

This observation causes the translation of classifications to LOR to involve both quantitative and qualitative goals. This is best stated in Part 1 of IEC 61508:

> *It is important to note that the failure measures for SILs1, 2, 3 and 4 are target failure measures. It is accepted that only with respect to the hardware safety integrity (see 3.5.5 of IEC 61508-4) will it be possible to quantify and apply reliability prediction techniques in assessing whether the target failure measures have been met. Qualitative techniques and judgements have to be made with respect to the precautions necessary to*

Figure 4.2. Software Criticality Matrix
This figure shows how the severity and software control categories are correlated to determine a software criticality index for the DOD (Table 4-2 of Ref [1])



[A] One SIL 3 E/E/PE safety-related system does not provide sufficient risk reduction at this risk level. Additional risk reduction measures are required.
[B] One SIL 3 E/E/PE safety-related system may not provide sufficient risk reduction at this risk level. Hazard and risk analysis is required to determine whether additional risk reduction measures are necessary.
[C] An independent E/E/PE safety-related system is probably not required.
[D] Event likelihood is the likelihood that the hazardous event occurs without any safety related systems or external risk reduction facilities.
[E] SRS = safety-related system. Event likelihood and the total number of independent protection layers are defined in relation to the specific application.

Figure 4.3. Hazardous Event Severity Matrix
This example figure shows how the number of safety related systems and the severity are correlated to identify the SIL that should be required within the IEC 61508 and ISA 84.00.01 framework (Figure E.1 of Ref [36])

meet the target failure measures with respect to the systematic safety integrity (see 3.5.4 of IEC 61508-4) [32].

As an example of this, each SIL is assigned a quantitative reliability goal (as shown in Figure 4.4) but is also given an extensive set of recommended and highly recommended design criteria in Parts 2 & 3 of IEC 61508 [15], [24] and Part 1 of ISA 84.00.01 [16].

A useful comparison of LOR is difficult partly because the DOD has set up their process to utilize a custom tailored LOR for each project that correlates the SCI to specific tasks through the different phases of the development process, as shown in Figure 4.5. Each DOD project could potentially have very different definitions of what is involved with the same category of a level of rigor.

The level of rigor is defined in the international nuclear industry quite well through the IEC nuclear standards. The A, B, and C categories are threaded throughout the associated standards so that the efforts applied to hardware and software are laid out clearly for each of those categories. It is quite the opposite of the DOD's custom tailored level of rigor framework.

The US nuclear industry has a clearly defined level of rigor at the system level, but because the framework only contains two categories, the level of rigor at the individual component level is vague. A prime example of this is in commercial grade dedication of digital components. In the guidance and standards associated with this type of activity it is commonly stated that the level of rigor should be determined based on the "safety significance and complexity of the device" [28]. This is identified as a "Graded Approach" [2]. The problem with this guidance is that it is very open ended. There is no clear definition of the scales for safety significance and complexity, and there is also no clear translation of those factors into specific levels of effort. This industry recognizes this issue and continues to work towards resolving it.

A detailed review and comparison of levels of rigor for each classification scheme would be necessary to positively correlate each of them to the IEC 61508 SILs. This task is possible but would require a substantial amount of time and effort. For the purposes of this thesis, this correlation will not be made. Instead it will suffice to acknowledge that the correlation is possible to be made and to categorize that effort as potential future work. Because of the customization of LORs for the DOD, correlation in that scheme would simply be that IEC 61508 SILs would be integrated into custom sets of LORs.

Defending Against Random Failures

Hardware

Random failures of individual hardware components are typically not attributed to design flaws but instead are the result of variations in the manufacturing process and the specific environmental stressor a component is exposed to. At some level, these failures are simply accepted as being inevitable.

Safety integrity level	High demand or continuous mode of operation (Probability of a dangerous failure per hour)
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

Figure 4.4. SILs
Qualitative reliability goals specified within the IEC 61508 framework (Table 3 in Section 7.6.2.9 of Ref [32])

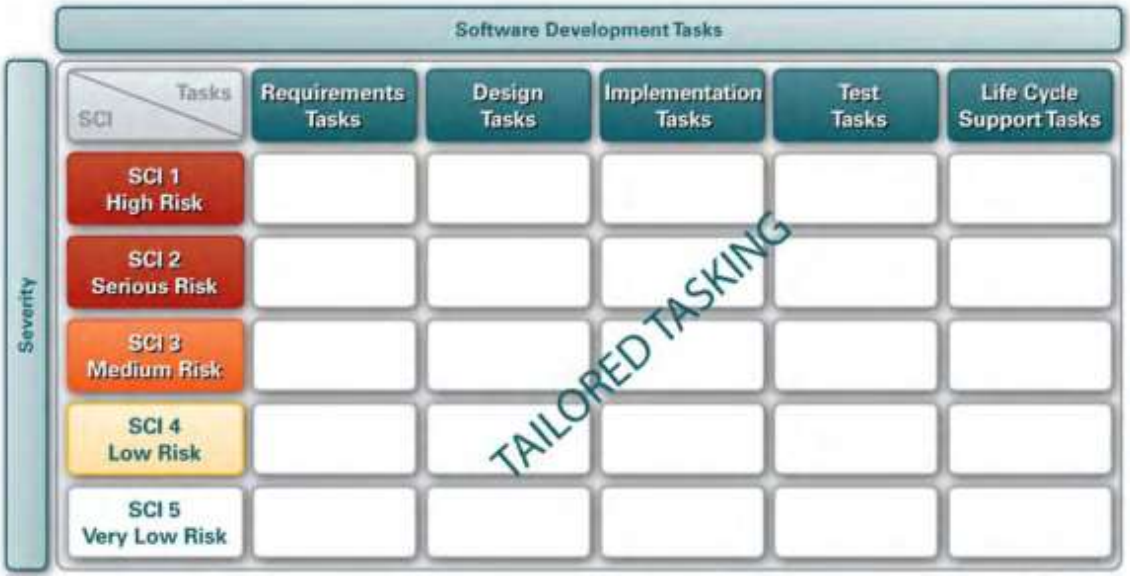


Figure 4.5. Example Custom LOR Template
This is an example of how levels of effort are customized within DOD projects to meet project specific requirements (Figure 4-13 of Ref [1])

Efforts are certainly made to use the longest lasting and most reliable components, but at some point the focus must be put on designing systems so that they can handle these random hardware failures when they occur. The actual techniques implemented vary between the industries that have been surveyed. For additional background information on reliability see references [65], [66].

Both the US and international nuclear industries, through utilizing IEEE standards and IAEA safety guides, implement a defense in depth strategy that generally starts with a methodology called the single-failure criterion [11], [67]. The single-failure criterion is a deterministic approach to a hardware system reliability analysis. In this strategy, the system is designed in a manner that no single component failure can cause the system to fail from performing its safety function. This criterion covers the potential cascading failures and the failures resulting from design basis events, such as earthquakes. Particularly for computer based systems, this criterion includes the failure of a single control processor or a single software fault [17], [67].

One critique of this methodology is that due to its deterministic nature and its system level focus, it is difficult to clearly identify what the reliability targets should be for individual components within the system. It is assumed that no more than one independent failure will occur within the system at a time, so probabilistic and quantitative methods can be implemented to help ensure this goal is achieved [23], [67]. While there appears to be a common intention among countries with nuclear power plants to increase the use of probabilistic and quantitative reliability goals [67], [68], the actual level of implementation is at varying degrees.

In the nuclear industry, redundancy is the key technique used to defend against random failures. The use of redundancy is how the single failure criterion is complied with. The idea of redundancy is that additional replicated paths are available for the accomplishment of the safety function that the system is required to perform. The secondary factor that is considered in conjunction with redundancy is independence. Redundancy can only be effective if the replicated paths are sufficiently independent of each other.

Redundancy and independence are intended to be applied into the overall design of the system but it is possible for them to be included internally to complex components. It is not commonly expected for that to be the case for off-the-shelf equipment. A more common expectation for typical components is that they will be of high quality to allow for the achievement of a qualitatively high level of reliability.

In contrast to the nuclear industry, both the DOD and the process industry mainly utilize probabilistic approaches to defend against random failures. Both qualitative and quantitative methodologies are used but the risk or likelihood of a failure is consistently included [1], [14], [16]. Some of the techniques commonly used are reliability block diagrams, Markov modeling, fault tree analysis, and failure mode and effects analysis [69]. Typically one or a combination of these

methods is used to model the system, commonly in a quantitative manner, to determine if the system will provide the required level of reliability. When performed quantitatively, a numerical value of reliability is assigned to the individual components so that they can be analyzed together to determine a numerical value for the overall system. These modelling approaches, even when performed qualitatively, tend to make it easier to derive reliability goals for individual components than it is when deterministic approaches, such as the single failure criterion, are used [69].

Despite the differences in deterministic and probabilistic system reliability analysis techniques, the approach to defending against random failures is very similar to what is done in the nuclear industry. Redundant system architectures are once again the key. In the process industry the term often used is fault tolerance [16]. Redundancy is the primary methodology for designing fault tolerance into systems. A specific example of how redundancy can be built in to increase fault tolerance is in the use of voting schemes. Independent sections can be setup to be compared to determine the state of a process and to diagnose failures within the redundant sections. In these designs, the control logic is configured to take action based on the state of one or multiple input signals (the redundant signals are considered to be voting for a particular action to occur or not occur). One out of two (1oo2) and two out of three (2oo3) architectures are commonly used depending on if the goal is to achieve high reliability, or high availability, or both [69].

Software

In general, random failures are not considered to be applicable to software. Software-related issues are typically characterized as systematic failures, and therefore, are not generally analyzed within reliability assessments. Within the industries surveyed there were no measures identified to defend against random failures of software. There is no common implementation of concepts such as hardware redundancy when it comes to software. There is a similar concept called diversity [11], [67] that is commonly used but from a rigorous perspective, diversity is an approach to prevent systematic faults. Therefore, it will not be discussed here, but instead, will be found in the next section.

Preventing Systematic Faults

Beyond the random hardware failures, the other issue that must be addressed is systematic faults. These are design errors that were not observed and corrected during the development process. In order to prevent these kinds of faults from being allowed to exist within the design of a component or system, rigorous methods have been developed to be used during the design process.

Lifecycle Processes and Designing Techniques

The main frame work that is applied to prevent systematic faults is the lifecycle methodology and the designing techniques that are interwoven into the phases of the lifecycle. The use of a lifecycle methodology is a common practice between all of the industries surveyed. Within the IEC 61508 standards, implemented within the process industry, and utilized in the international nuclear industry, is an overall safety system lifecycle, as shown in Figure 4.6. This structure is broken down into more detail for the system hardware and software realization phase as shown in Figure 4.7 and Figure 4.8. Then Figure 4.9 shows a design process lifecycle approach from IEEE 1012 (Standard for System and Software Verification and Validation) which is a commonly used standard in the US nuclear industry. Common among the life cycle models for the realization of equipment is that they will start with a phase that captures the requirements that will become the goals for the design to achieve. Then there is generally a phase were the requirements are translated into a plan for the hardware and software design. Next there is typically a phase for implementing the design plan by building the hardware, writing the software code, and then integrating the hardware and software together. Finally, a validation phase is generally utilized to take measures to prove that the requirements established at the beginning of the process have been met. The different models contain these phases, as a minimum, and will vary in what other phases are also included, such as periodic hazard analysis. The models also vary in how the process is expected to move between the different phases. Some examples of this potential difference can be seen from DOD standards and are shown in Figure 4.10 and Figure 4.11. The reason that lifecycles have been broadly implemented across these different industries is that it is a common perspective that they facilitate a very methodical process which causes the design team to focus on making sure that they fully accomplished what they set out to do.

Built-in Safety Features

There are many features that can be included within the design of a component to increase its ability to operate safely and reliably. Many of these types of design features fall into the category of being self-diagnostics. Self-diagnostics and fault detection are features that are included within the design that provide immediate identification of when there is a problem. It was observed universally through all the industries surveyed that these types of features were desirable to be included. One specific example for why this is important is the topic of fault detection [17]. One of the worst scenarios for a safety system is that it is in a failed state and there is no indication of a problem until the system is called upon to perform its safety function.

Throughout the industries surveyed, specific techniques for self-diagnostics and fault detection are typically not specified, but instead, the requirements specify that these types of features shall be included. In this context, it is typical for best practices to be complied and included as reference

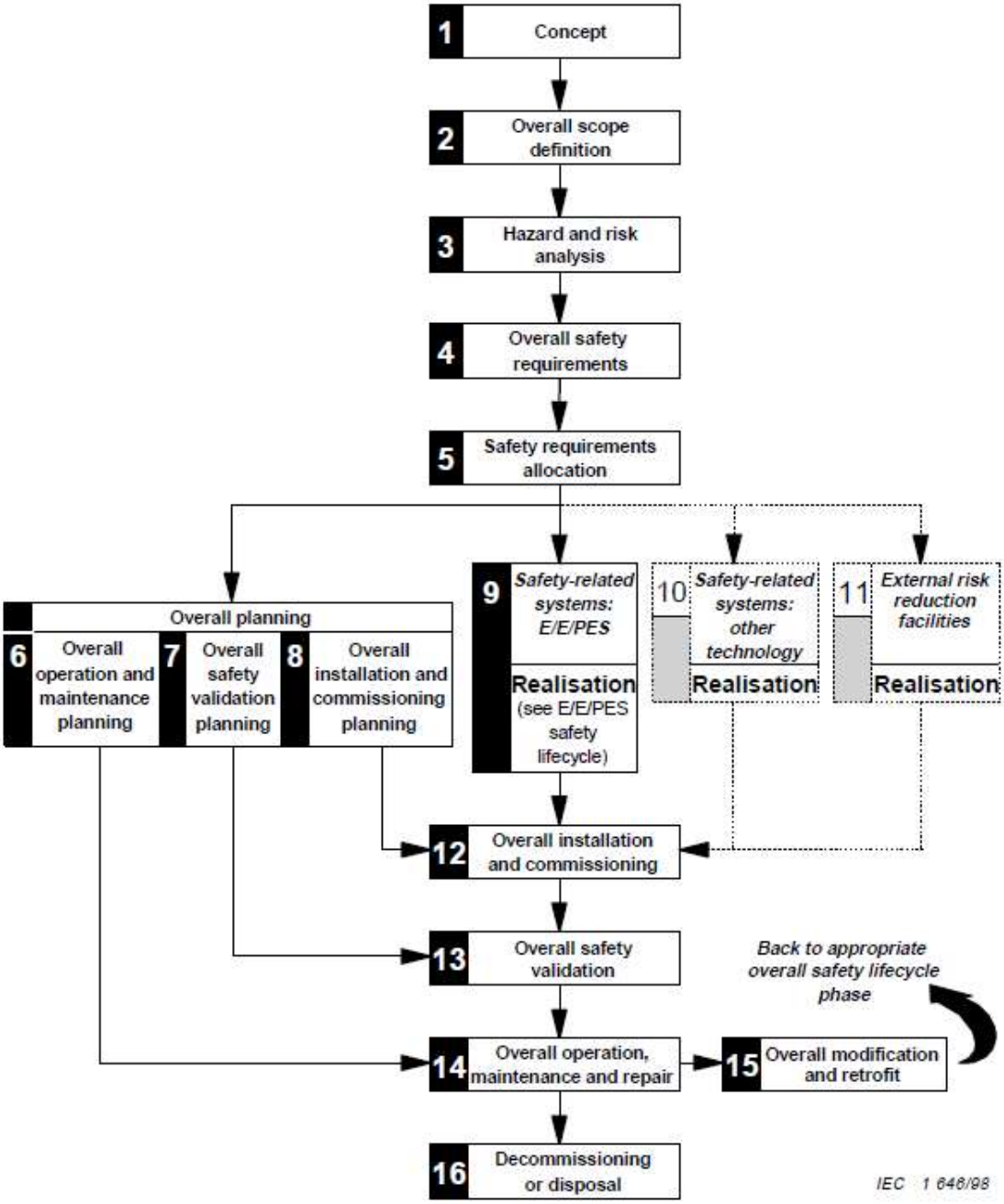


Figure 4.6. Overall Safety Lifecycle
This figure presents the full lifecycle covered by the IEC 61508 framework. This is at the plant level and is filtered down into individual lifecycles of specific safety systems and equipment (Figure 2 of Ref [32])

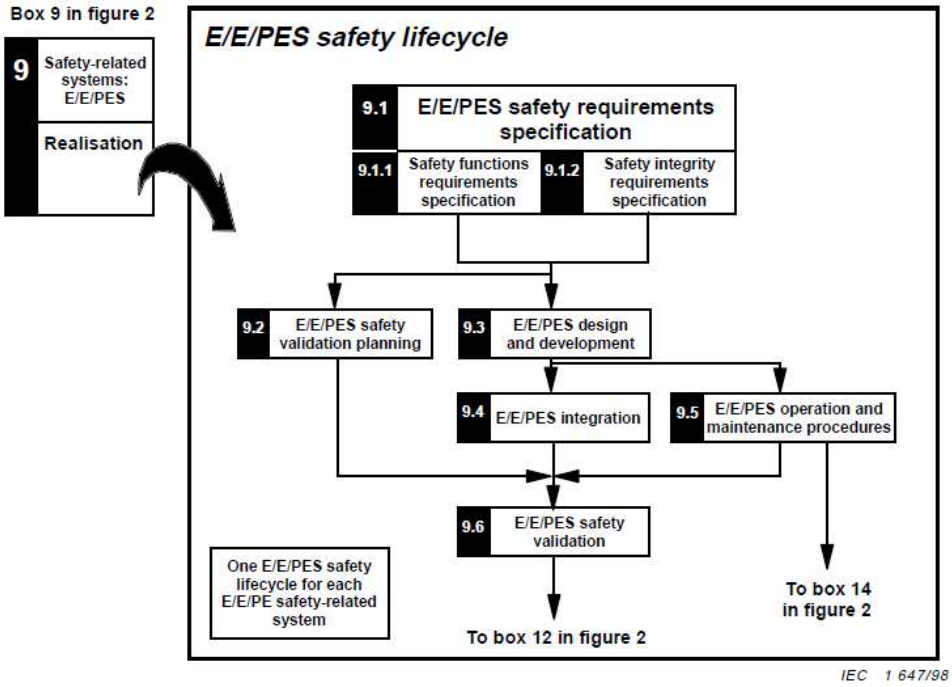


Figure 4.7. Safety Lifecycle- Equipment Realization Phase
This is the section of the IEC 61508 lifecycle that applies to the realization of individual systems and/or components (Figure 3 of Ref [32])

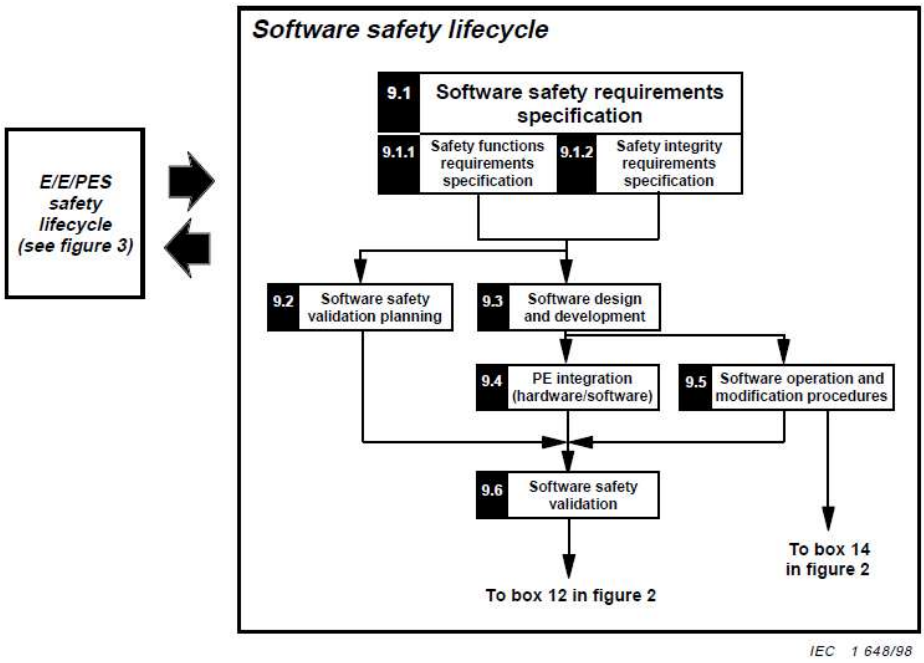


Figure 4.8. Safety Lifecycle- Software Realization Phase
This is the section of the IEC 61508 lifecycle that applies to the realization of the software for individual systems and/or components (Figure 4 of Ref [32])

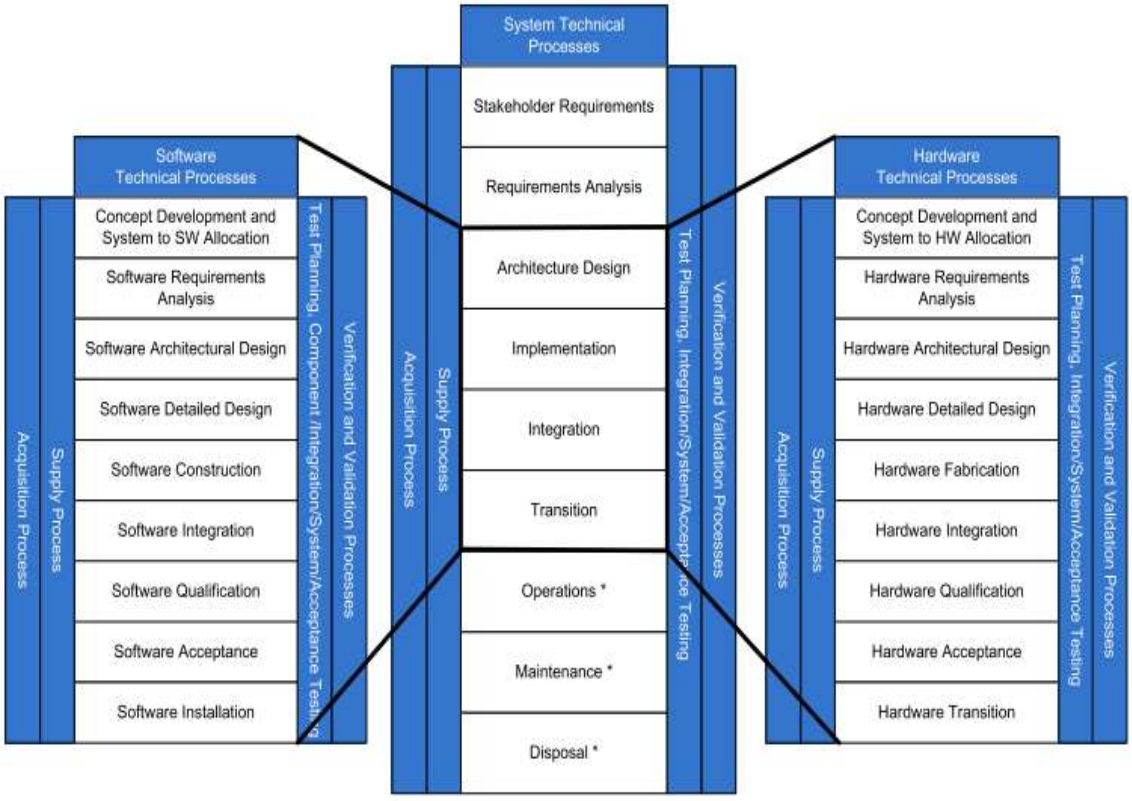


Figure 4.9. Relationship of system, software, and hardware processes
This illustrates development process within the IEEE structure and shows the relationship between the overall design process, the hardware design process, and the software design process (Figure 5 of Ref [70])

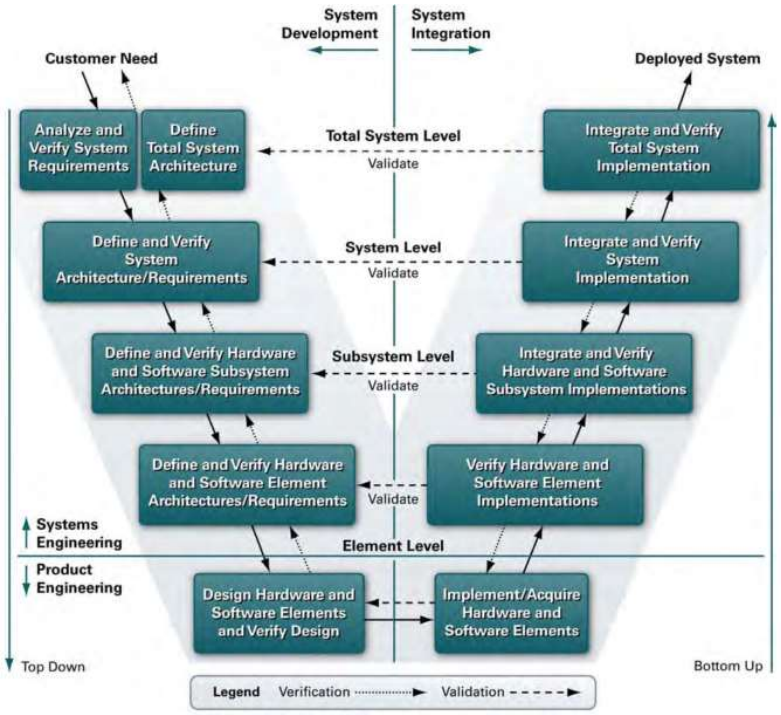


Figure 4.10. V Model
This illustrates the V model of verification and validation used in DOD projects. It is commonly used outside the realm of DOD projects as well (Figure 2-6 of Ref [1])

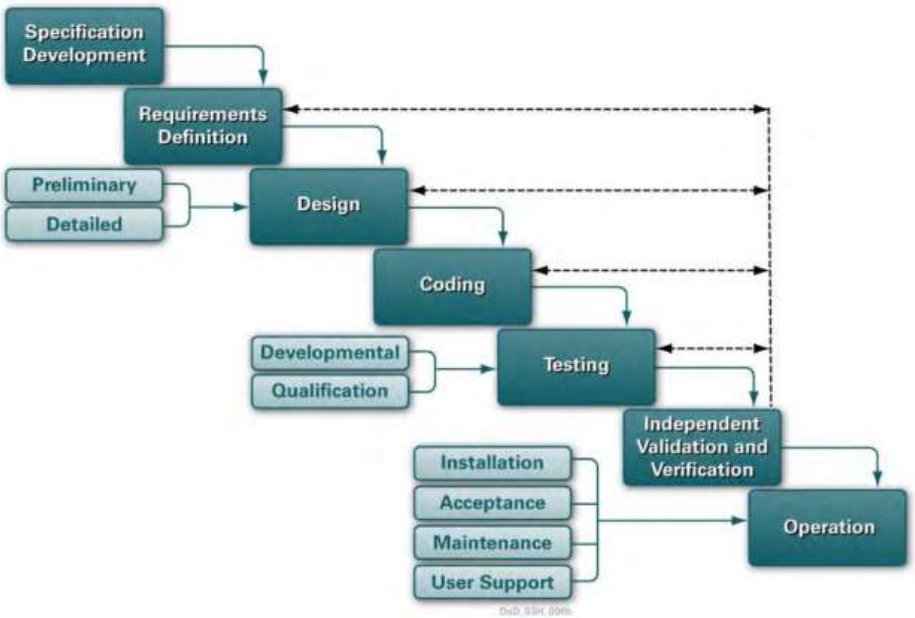


Figure 4.11. Grand Design Waterfall Model
This illustrates the Waterfall model of verification and validation used in DOD projects. It is commonly used outside the realm of DOD projects as well (Figure 2-5 of Ref [1])

material to aid the designers in choosing the features that integrate the best into their overall design [1], [38]. In other contexts specific percentages of coverage are specified to drive the reduction of the probability of the existence of an undiscovered failure [15].

Design Analysis and Verification & Validation

Within the lifecycle processes, there are a variety of techniques that may be used to perform design analyses and to perform verification and validation testing that may pertain to hardware, software, or both. These aspects are considered vital to the development of safety systems and components in order to ensure the design meets all the specified requirement. These topics are consistently addressed at a high level within the standards of the industries surveyed. The specific techniques to be utilized are generally left open to be determined by the designers/ engineers of the equipment, but some are identified as recommended or highly recommended for particular levels of rigor (also known as integrity levels).

Parts 2, 3, and 7 of the IEC 61508 standard for functional safety [15], [24], [38] contain comprehensive appendices that identify a wide range of these analysis and testing techniques. The techniques are provided in a tabular format which includes insight into how the classification of the equipment and the corresponding level of rigor (a.k.a. integrity level) are factored in. Figure 4.12 and Figure 4.13 are examples of these types of tables taken directly from these standards. These appendices are potentially very useful for interfacing between industries and equipment manufacturers to ensure expectations of the rigor to be applied in the prevention of systematic faults is clearly understood by both parties involved.

The document that best addresses this topic area in the US Nuclear industry is IEEE 1012 [70]. This standard addresses testing of individual components, at the integration phase, at the qualification phase, and at the acceptance phase. Some of the types of design analyses discussed are algorithm analysis, control flow analysis, data flow analysis, simulation analysis, and code sizing and timing analysis.

For the US DOD, the Joint Software System Safety Engineering Handbook [1] identifies many potential techniques that could be used for analysis and testing. A sample of what is include is data flow analysis control flow analysis, “What If” analysis, interface analysis, safety-critical path analysis, thread analysis, interrupt analysis, requirements-based testing, path coverage testing, stress testing, endurance testing, and fault insertion and failure mode testing.

Hazard Analysis

Another methodology that is used to prevent systematic faults is the hazard analysis. A hazard analysis is defined as “A process that explores and identifies conditions that are not identified by the normal design review and

	Technique/measure	See IEC 61508-7	SIL1	SIL2	SIL3	SIL4
	Observance of guidelines and standards	B.3.1	HR mandatory	HR mandatory	HR mandatory	HR mandatory
	Project management	B.1.1	HR low	HR low	HR medium	HR high
	Documentation	B.1.2	HR low	HR low	HR medium	HR high
	Structured design	B.3.2	HR low	HR low	HR medium	HR high
	Modularisation	B.3.4	HR low	HR low	HR medium	HR high
	Use of well-tried components	B.3.3	R low	R low	R medium	R high
	Semi-formal methods	B.2.3, see also table B.7 of IEC 61508-3	R low	R low	HR medium	HR high
	Checklists	B.2.5	– low	R low	R medium	R high
	Computer-aided design tools	B.3.5	– low	R low	R medium	R high
	Simulation	B.3.6	– low	R low	R medium	R high
	Inspection of the hardware or walk-through of the hardware	B.3.7 B.3.8	– low	R low	R medium	R high
	Formal methods	B.2.2	– low	– low	R medium	R high

Figure 4.12. Example from Appendix B of Ref [15]
This is an example of the content of Appendices A, B, and C of Part 2 of IEC61508 and shows how SILs are easily and clearly translated into specific levels of effort in the design process

(This includes software system design, software module design and coding)

	Technique/Measure*	Ref	SIL1	SIL2	SIL3	SIL4
1a	Structured methods including for example, JSD, MASCOT, SADT and Yourdon	C.2.1	HR	HR	HR	HR
1b	Semi-formal methods	Table B.7	R	HR	HR	HR
1c	Formal methods including for example, CCS, CSP, HOL, LOTOS, OBJ, temporal logic, VDM and Z	C.2.4	---	R	R	HR
2	Computer-aided design tools	B.3.5	R	R	HR	HR
3	Defensive programming	C.2.5	---	R	HR	HR
4	Modular approach	Table B.9	HR	HR	HR	HR
5	Design and coding standards	Table B.1	R	HR	HR	HR
6	Structured programming	C.2.7	HR	HR	HR	HR
7	Use of trusted/verified software modules and components (if available)	C.2.10 C.4.5	R	HR	HR	HR

* Appropriate techniques/measures shall be selected according to the safety integrity level. Alternate or equivalent techniques/measures are indicated by a letter following the number. Only one of the alternate or equivalent techniques/measures has to be satisfied.

Figure 4.13. Example from Appendix A of Ref [24]
This is an example of the content of Appendices A, B, and C of Part 3 of IEC61508 and shows how SILs are easily and clearly translated into specific levels of effort in the software design process

testing process. The scope of hazard analysis extends beyond plant design basis events by including abnormal events and plant operations with degraded equipment and plant systems. Hazard analysis focuses on system failure mechanisms rather than verifying correct system operation" [71]. There are several ways to perform a hazard analysis and there are several different points in projects when they can be utilized.

The US DOD implements hazard analyses at many points in their projects. They perform a preliminary hazard analysis, a system requirements hazard analysis, a subsystem hazard analysis, a system hazard analysis, an operating and support hazard analysis, a health hazard analysis, a functional hazard analysis, a system-of-systems hazard analysis, and finally an environmental hazard analysis [14]. They utilize all of these iterations of analysis to continuously evaluate risk of systematic faults and make as much effort as is appropriate to reduce or eliminate that risk.

The process industry uses what they call a failure analysis but it is essentially the same thing as a hazard analysis and is used in the same way as how hazard analysis has already been defined. The types of failure analysis identified in the IEC standards typically used by the process industry are the failure modes and effects analysis, cause consequence diagrams, event tree analysis, failure modes, effects and criticality analysis, fault tree analysis, worst-case analysis, expanded functional testing, worst-case testing, and fault insertion testing. Many of these types are found in the other industries surveyed as well, possibly identified as failure analysis or hazard analysis techniques.

The US nuclear industry identifies the following guidelines for the implementation of hazard analysis: avoidance of hazards identification and evaluation of hazards, identification of hazards throughout the system life cycle, resolution of hazards, evaluation of hazards in previously developed systems, and documentation of hazard analysis plans, responsibilities, and results [17].

Common Cause Failure Prevention

Despite the rigorous effort put into ensuring that no systematic faults exist within safety systems, preventative measures are also implemented for dealing with the design errors that may potentially be introduced. One of the types of systematic faults that get a lot of attention in the process and nuclear industries is common cause failure. Simply put, common cause failures are design flaws that can cause multiple redundant sections of a safety system to all fail at the same time. This type of failure is of concern because by itself it can defeat several layers of defense against failure with one event. An example is a vulnerability to radiated electromagnetic interference. If an identical component is used in every redundant path of the safety system and then they all fail due to a technician using a radio for communication in their vicinity the overall system just failed due to one cause [69].

To prevent potentially unidentified common cause failures from defeating the safety system, diversity and independence are worked into the redundant

sections of the system. Diversity is defined as, “the principle of monitoring different parameters, using different technologies, different logic or algorithms, or different means of actuation in order to provide several ways of detecting and responding to a significant event” [67]. This means that redundant sections of the system will utilized entirely different technologies, they may monitor entirely different parameters of the process, and they may actuate safety functions in entirely different ways. Independence is the principle of the redundant and diverse sections of the system functioning separate from each other in as many ways as possible. For example, the different sections of the system should not both be dependent on the same power source. “Independence prevents: (1) propagation of failures from system to system or (2) propagation of failures between redundant parts within systems, and (3) common cause failures due to common internal plant hazards” [67].

The process industry also considers common cause issues. The guidance in that industry for avoiding common cause failures is 3 principles. Principle 1 is to reduce common stress, principle 2 is to apply diversity, and principle 3 is to ruggedize the design for high strength [69].

Within the US nuclear industry, it is understood that systems need to be designed to be protected from unidentified common cause failures. A specific analysis technique has been developed and put into practice for the purpose of identifying those potential failures. This analysis is called diversity and defense-in-depth and is often abbreviated as D3. What D3 is intended to do is to identify if a safety system has enough diversity or not. Diversity can be implemented to varying degrees and in various ways. To promote consistency, standards such as IEEE 7-4.3.2 include requirements for the level of diversity that must exist and research has been performed to better identify the different approaches that can be utilized. The NRC published that research in NRC CR-7007 “Diversity Strategies” and this document identifies 3 separate strategies that can be utilized. Those strategies are defined as:

> *Strategy A- focuses on the use of fundamentally diverse technologies as the basis for diverse systems, redundancies, or subsystems. The Strategy A baseline, at the system or platform level, is illustrated by the example of analog and digital implementations providing design diversity. This choice of technology inherently contributes notable equipment manufacturer, processing equipment, functional, life-cycle, and logic diversities. Intentional application of life-cycle and equipment manufacturer diversities is included in the baseline, while the traditional use of functional and signal diversities is also adopted. The use of a microprocessor-based primary protection system and an analog secondary protection system at the Sizewell NPP represents the principal example of Strategy A drawn from the survey findings.*
>
> *Strategy B- involves the use of distinctly different technology approaches as the basis for diverse systems, redundancies, or subsystems. The Strategy B baseline can be described in terms of*

different digital technologies, such as the distinct approaches represented by programmable logic devices and general-purpose microprocessors. This choice of technology inherently contributes some measure of equipment manufacturer, processing equipment, functional, life-cycle, and logic diversities. Intentional application of logic processing equipment, life-cycle, and equipment manufacturer diversities is included in the baseline, while the traditional use of functional and signal diversities is also adopted. The Olkiluoto diversity approach using different digital technologies (i.e., CPUs vs FPGAs) as the basis for the primary safety system and a diverse backup system is the principal example of Strategy B drawn from the survey findings. Nonnuclear industry examples from the rail industry employed this technology difference to implement significantly different functional approaches in a parallel arrangement of safety-critical and checking systems.

Strategy C represents the use of architectural variations within a technology as the basis for diverse systems, redundancies, or subsystems. An example of the Strategy C baseline involves different digital architectures, such as the diverse microarchitectures provided by different CPUs. This choice of technology inherently contributes some limited degree of equipment manufacturer, life-cycle, and logic diversities. Intentional application of equipment manufacturer, logic processing equipment, life- cycle, and logic diversities is included in the baseline, while the traditional use of functional and signal diversities is also adopted. The use of diverse microprocessors as the basis for primary safety systems and diverse backup systems such as (ATWS) or (DAS) constitutes the principal examples of Strategy C drawn from the survey findings. Nonnuclear industry examples primarily involve flight control systems for the aviation industry. [72]

Environmental Qualification

Environmental testing is used in the nuclear industries to detect potential systematic faults and common cause failures by exposing the equipment to worst case conditions for what they could see while in service. During this testing, the equipment is verified to successfully perform their safety function before, during, and after exposure to the anticipated conditions [43], [55]. This testing is typically extended out to all credible design basis events for the reactor site and often involves seismic testing, radiation exposure, aging analysis, and extreme electromagnetic compatibility testing. This technical aspect appears to be one significant difference between the nuclear industry and the process industry in that the process industry does not typically require the same kinds of environmental qualification and does not invoke the same level of rigor. As a result, the typical safety certified off-the-shelf equipment utilized by the process industry may be lacking in this area when attempted to be used in the nuclear industry.

Suitability Evaluation of "Off-the-Shelf" Equipment

In any industry, once an I&C safety system has been conceptually specified and designed the inevitable next question is, will new equipment need to be created or is there equipment already in existence that could be utilized? There can be several factors that go into answering this question. Factors such as how close does existing equipment come to meeting the conceptual requirements, what is the cost difference between using something existing versus creating something new, will this be a one of a kind system or will several copies be needed, can new equipment be as dependable as existing mature products. These factors can play out very differently in each industry and in the variety of applications, but inevitably the need arises to evaluate existing equipment (often called off-the-shelf equipment) for use in safety systems.

There are several common threads between the each industry's processes of evaluating the suitability of off-the-shelf equipment. All of the industries surveyed would focus on determining the functional suitability of the potential equipment (does it adequately perform the functions that are required), and then a deeper look is taken at the design processes that were used to be able to prove that the item has sufficient design integrity to prove the required reliability and assurance that there is built in quality to prevent systematic faults. It is also common to review operating history of potential products to mitigate deficiencies in design documentation. This is sometimes referred to as the prior use basis, and is simply making the claim that since the component operated successfully in the past in applications that are similar to the proposed application, there is reasonable assurance that it will also operate successfully in that proposed application [1], [15], [28]–[30].

An aspect of all suitability evaluations is that they consist of two parts. The first part is an analysis of the intended application. The second aspect is the analysis of the potential equipment. This seems to be common sense as it is necessary to understand both aspect to be able to make a credible determination. For the purposes of this thesis, the application specific aspects will be omitted since every application is different and the intent of the safety certification process is to provide a generic assessment that can be utilized for many applications.

There are two documents that service as good examples of these concepts and commonalities. The first is IEC 62671, [30] from the international nuclear industry and is focused on equipment of limited functionality. The second is EPRI 1011710, [29] from the US nuclear industry, and is typically applied to complex equipment.

A summary of the topics addressed in IEC 62671 is Competence of Primary Function, Ancillary Functions, Configurability, Superfluous Functions, Hardware Robustness, Reliability, Maintainability, and Testability, Cybersecurity, User Documentation for Safety, Previous Certification, Avoidance of Systematic Faults, Evidence of Quality in the Design Process, Evidence of Quality in Manufacturing, Product Stability, Operating Experience, Complementary Testing

and/or Analysis, and Documentation Improvement. A summary of the EPRI 1011710 format is a Functional Review, an Architecture Review, a Process Review, a System Failure Analysis, and an Operating History Survey.

Synthesis of Observations

As a result of this comparing and contrasting activity, the point can be made that, at the system level, there are significant and possibly irreconcilable differences between the surveyed industries. Particularly because of the topics of hardware reliability and common cause failure prevention, it may be too large of a task to attempt to repurpose an entire system from an application in one of these industries for use in another. But, in contrast, a case can be made that many of these significant differences fade away as the perspective is lowered from the system level to the individual component level. The term component is used to refer to a typical piece of industrial equipment, such as a sensing element, a logic solver, or a control element.

Classification scheme differences at the system level could be highly impactful to the compatibility of that system to another industry. Classification is a foundational aspect that drives the level of rigor of all the activities that go into developing and implementing the system. Variability at that level will have significant rippling effects between all the interfaces involved. At the component level the impact of classification differences and the resulting variability of level of rigor can be better understood and evaluated since the scope of the design under consideration is much simpler.

Within the realm of the defense against random hardware failures, the system level concept of single failure criterion is difficult to correlate with probability based reliability methodologies. But at the component level of the single failure criterion methodology, the requirements are very loose and easily compatible with other quantitative probabilistic reliability methodologies. Since the goal of the single failure criterion is to ensure that no one failure can prevent the system from performing its safety function, the reliability requirements of the individual components boils down to each one being reliable enough to provide reasonable assurance that when one failure occurs that there is sufficient time for that failure to be repaired before the next failure happens. This scenario could easily be translated into a standard quantitative value to be applied to each individual component.

The use of lifecycle processes was a topic where no major differences were observed and these processes are generally very scalable between the system and component levels. The lifecycle of the overall system typically wraps around and encompasses the lifecycle processes of the individual components.

The topics of built-in safety features, design analysis, verification, and validation, and hazard analysis are similar to the topic of lifecycle processes, in regards to their impact to the system and component levels. None of these present significant negative impact to efforts to utilize the same systems or components in various industries.

Common cause failure prevention is very application specific and the level of rigor that was observed being applied to this activity did vary significantly between the different industries. This topic focuses on redundancy, independence, and diversity at the system level and the nuclear industry seems to have focused in on it more than the US DOD or the processes industries. There are many different possible approaches to this type of prevention as previously discussed, but similarly to what was observed regarding other cases of significant system level differences, when the perspective is lowered down to the component level the significance of those differences fade away. At the component level, the only considerations of this topic are documentation of the design architecture and processes to ensure the necessary information is available when the common cause failure prevention activities occur at the system level. Other than that there is little to be concerned with when evaluating an individual component.

It is ideal to evaluate environmental qualification at the system level but it is reasonable to conclude that a system assembled with individual components that are qualified for the specified environment will also be able to be qualified for that same environment. Dealing with this topic at the individual component level may result in some level of over qualification because of testing being performed without components installed within cabinets and a lack of ability to evaluate anomalous behavior within the context of the system, but as long as it is economically feasible to accomplish, it would not be an issue that would prevent the exchangeability of equipment from one industry to another. The current reality of this subject is that components are typically qualified to environmental parameters that are normal for most process industries and do not encompass the extremes that are sometimes experienced in the nuclear industry or in DOD applications, making this topic the most significant negative impact to be able to use the same components universally between different industries.

Within suitability evaluations of “off-the-shelf” equipment, no significant differences were observed so no significant negative impact to efforts to utilize the same systems or components in various industries were perceived. In practice, this is a topic that mainly applies to individual components, but technically it could be used for systems so it was additionally observed that the suitability evaluation processes would be applied similarly at both the system and component levels.

As a result of these observations, it is clear that the greatest potential for a standardization of functional safety requirements and assessments between the various industries and equipment manufacturers is at the component level and not at the system level. The observations have been summarized in those components being suitable for use within many different systems and applications. The components can be common to the various industries, and the specific requirements of the different industries can be met as the components are integrated together into the complete system.

Table 4.1. The indication of “Low” in the last column of that table supports the determination of the standardization of functional safety being implemented at the component level. It can be concluded that most of the significant differences between the industries’ equipment requirements fades away down at the individual component level. This means that there is potential for manufacturers to focus on those components being suitable for use within many different systems and applications. The components can be common to the various industries, and the specific requirements of the different industries can be met as the components are integrated together into the complete system.

Table 4.1. Comparison of System and Component Levels
This table summarizes the significance of the observed differences regarding the specified topics at both the system and individual component levels. The indication of “Low” in the last column supports the determination of the standardization of functional safety being implemented at the component level.

Category	Significance of Differences at the System Level	Significance of Differences at the Component Level
Classification Schemes		
• Probabilistic vs Deterministic	High	Low
• Level of Rigor	High	Low
Defense against Random Hardware Failures	High	Low
Preventing Systematic Faults		
• Lifecycle Processes	Low	Low
• Built-in Design Safety Features	Low	Low
• Design Analysis, Verification, and Validation	Low	Low
• Hazard Analysis	Low	Low
• Common Cause Failure Prevention	High	Low
• Environmental Qualification	High	High
Suitability Evaluations of “Off-the-Shelf” Equipment	Low	Low

CHAPTER FIVE

STANDARDIZATION OF COMPONENT FUNCTIONAL SAFETY

As concluded in the previous chapter, there is significant potential for standardization of functional safety requirements and assessments between various industries and equipment manufacturers at the component level. The vehicle proposed for use in this manner is the IEC 61508 set of standards accompanied by an independent certification process. Using the criteria and topic areas identified in the previous chapter, some actual “off-the-shelf” components will be evaluated to demonstrate how manufacturers have produced equipment that can be suitable for various safety significant applications in various industries by voluntarily seeking compliance with IEC 61508. To that end, the categories identified in the previous chapter will be used as criteria for evaluation of components. Showing that components adequately comply with these criteria will demonstrate their ability to be used in multiple industries, based on the discussions in the previous chapter.

Additionally, these evaluations will seek to show how industries can avoid significant risk and remove uncertainty when embarking on a suitability evaluation of “off-the-shelf” equipment by intentionally engaging with manufacturers who have voluntarily sought and achieved third party certification to IEC 61508 to SIL 2 or higher. SIL 1 is excluded because at that level, some uncertainty about the design and manufacturing processes remains due to the greater potential for the “proven in use” basis to be utilized. To achieve SIL 2 or higher it can be more reasonably assumed that the original development activities included intentional efforts to seek compliance with IEC 61508.

It is to these two ends that the following evaluations are being conducted, to show the practicalities of IEC 61508 as the vehicle for driving standardization, and also to show the higher level of confidence that can be reasonably assumed when making the initial decision to evaluate such equipment for suitability.

Please note that all information used in these evaluations was available to the general public from either the manufacturer’s website or from the Safety Automation Equipment List website [39]. The first evaluation has been summarized in Table 5.1 and the second is in Table 5.2. Also note that the equipment shown in these examples are primarily used in the process industry but as a result of the proposed standardization, they could be used in the nuclear industry or potentially others as well.

Moore Industries STZ Transmitter

The first criterion is classification scheme and as previously discussed, classification is an industry specific activity to link risk to level of rigor related to providing and proving design integrity of a component or system. The SILs are not technically a classification scheme but they provide for a clear mechanism to

Table 5.1. Evaluation of MII STZ Transmitter
This table summarizes the evaluation of the STZ Transmitter's design and associated design activities in the context of the criteria identified earlier in this thesis.

Criteria	Relevant Design Information	Source of Information	Adequacy of Design
Classification Scheme	SIL 3 Capable	exida Certificate [73]	Highly Acceptable
Defense against Random Hardware Failures	• 171 Safe FITs • 166 Dangerous Detected FITs • 85 Dangerous Undetected FITs	exida Certificate [73]	Highly Acceptable
Lifecycle Processes and Designing Techniques	• Functional Safety Management (FSM) Plan • Safety Requirement Specification (includes identification of safety function) • System Architecture Design • Software Architecture Design • Software Data Flow Diagrams • Software Structure Diagrams • Software Sequence Diagrams • Lifecycle Verification Checklist • MII Quality Management System	exida Assessment Report [74]	Highly Acceptable
Built-in Safety Features	• Self-diagnostics • Fault detection • Configurable safe failed state Designed to detect faults in: • Software control flow • Software data flow	exida Assessment Report [74]	Highly Acceptable

Table 5.1. Evaluation of MII STZ Transmitter (Continued)

Criteria	Relevant Design Information	Source of Information	Adequacy of Design
Design Analysis, Verification, and Validation	• Hardware Verification for correctness & consistency • Fault Injection, Module, and Integration Testing • Static Analysis for compliance with coding standard • 100% test coverage of all functions, statements, and branches • Requirements traceability document utilized • One or more test cases for each safety requirement • Static and dynamic testing was utilized	exida Assessment Report [74]	Highly Acceptable
Hazard Analysis	Failure Mode, Effect, and Diagnostic Analysis (FMEDA)	exida Assessment Report [74]	Acceptable
Common Cause Failure Prevention	The details of the design are well documented and would be available as inputs to a system level assessment	exida Assessment Report [74]	Acceptable
Environmental Qualification	CE Mark, FM Approval Environmental qualification Operating Range: -40°C to +85°C (-40°F to +185°F) Storage Range: -40°C to +85°C (-40°F to +185°F) Relative Humidity: 0-95%, non-condensing 94/9/EC (ATEX) Explosive Atmospheres EMC qualification Directive: 2004/108/EC (EMC)	STZ User's Manual [75]	Good, But May Require Additional Industry Specific Attention
Suitability Evaluations of "Off-the-Shelf" Equipment	As a new product, successful operating experience will obviously be lacking but this can be mitigated by the extensive attention that has been paid to preventing systematic failures and extending the predicted FIT rate	exida Assessment Report [74]	Acceptable

Table 5.2. Evaluation of Fisher Controls DVC6200 Valve Controller

Criteria	Evidence	Source of Evidence	Measure of Adequacy
Classification Scheme	SIL 3 Capable (Digital Valve Controller Function)	exida Certificate [76]	Highly Acceptable
Defense against Random Hardware Failures	De-energize To Trip with Partial Valve Stroke Test • 582 Safe Detected FITs • 279 Safe Undetected FITs • 79 Dangerous Detected FITs • 41 Dangerous Undetected FITs Energize To Trip with Partial Valve Stroke Test • 487 Safe Detected FITs • 124 Safe Undetected FITs • 273 Dangerous Detected FITs • 94 Dangerous Undetected FITs	exida Certificate [76]	Highly Acceptable
Lifecycle Processes and Designing Techniques	• Functional Safety Management Plan • Lifecycle activities compliant with IEC 61508 • Safety requirement specification • Requirements traceability document • Hardware/ Software architecture specification • Detailed design description and design reviews • Detailed drawings and schematics • Checklists, semi-formal methods, computer aided design tools	exida Assessment Report [77]	Highly Acceptable
Built-in Safety Features	• Fault Detection • Backward recovery • Time-triggered architecture • Static resource allocation	exida Assessment Report [77]	Highly Acceptable

Table 5.2 Evaluation of Fisher Controls DVC6200 Valve Controller (Continued)

Criteria	Evidence	Source of Evidence	Measure of Adequacy
Design Analysis, Verification, and Validation	• Electrical unit testing • Hardware verification testing • Critical code reviews • Static source code analysis • Dynamic analysis • One or more test cases for each safety requirement • Unit testing • Functional testing • Fault injection testing • Black box testing	exida Assessment Report [77]	Highly Acceptable
Hazard Analysis	FMEDA	exida Assessment Report [77]	Acceptable
Common Cause Failure Prevention	The details of the design are well documented and would be available as inputs to a system level assessment	exida Assessment Report [77]	Acceptable
Environmental Qualification	CSA, FM, ATEX, IECEx, CUTR, INMETRO, PESO CCOE Electromagnetic Compatibility Vibration, Humidity, Explosion-proof, Flameproof	Instruction Manual [78]	Good, But May Require Additional Attention
Suitability Evaluations of “Off-the-Shelf” Equipment	There is indication that proven-in-use data is available for this item and it is not brand new so it is reasonable to expect significant and positive operating history data to exist for survey upon a more detailed evaluation.	exida Assessment Report [77]	Highly Acceptable

link to each industry's particular scheme. Future work is needed to map out the different classification schemes to specific SILs, but once that is done, the translation between classification and required SIL should be quite smooth. In this case, the exida certificate [73] indicates the Moore Industries Inc. (MII) STZ Dual Sensor Transmitter is SIL 3 capable. This means that industry specific applications would be able to easily determine if this item can be expected to be suitable based on what SIL level had been determined to be required.

The second criterion is defense against random failure. In the context of a single component it is expected that a quantitative goal will be required that will lead to the necessary reliability of the overall system. For this item, the overall failure rate was calculated in FITs (1 failure/ 1 billion hours), and the results were 171 Safe FITs, 166 Dangerous Detected FITs, and 85 Dangerous Undetected FITs [73] . These values could then be fed into the system level reliability analysis (deterministic or probabilistic) to ensure adequate reliability was going to be achieved.

The third criterion is lifecycle processes and designing techniques, which is a subtopic of preventing systematic faults. MII was found to have planned and implemented a safety life cycle that was in compliance with the requirements of IEC 61508 for a SIL 3 certification. The lifecycle activities were guided by a functional safety management plan. The Software Development Procedure identified the phases of the software development lifecycle and the inputs and outputs associated with each phase. The software design activities included the use of data flow diagrams, structure diagrams, and sequence diagrams. The documentation of the lifecycle and designing techniques provides clear understanding of what has occurred at the component level and also provides a clear transition of information and processes up to the system level.

The fourth criterion is another subtopic of preventing systematic faults. It is built-in safety features. The STZ transmitter has extensive self-diagnostics and fault detection features that were verified to have good coverage during the failure mode effect and diagnostics analysis (FMEDA). The software includes the ability to detect faults in the software control flow as well as in the data flow. Also the state in which the transmitter safely fails to is configurable to meet the needs of any specific application. This level of attention to developing a safe design at the component level will have a positive impact on efforts to design the overall system to function safely.

The fifth criterion is design analysis, verification, and validation, yet another subtopic of preventing systematic faults. The hardware of the STZ Transmitter has been verified to meet safety functions and safety integrity requirements. That verification has been demonstrated through testing and evaluation of the hardware phase outputs for correctness and consistency. The types of verification and validation that were used was fault injection testing, module testing, and integration testing. Testing was performed statically and dynamically. A static code analysis was performed on the source code to ensure compliance with coding standards. A requirements traceability document was

used to ensure that one or more test cases or analyses were used for validating each safety requirement.

This criterion is at the heart of what separates IEC 61508 certified components from the average commercial component. The design analysis and verification & validation activities that have been found to have occurred for this component are very important and helpful in establishing the safety integrity of the overall system. Formal activities of this type cannot be expected to exist for any typical commercial component.

The sixth criterion is hazard analysis, another subtopic of preventing systematic faults. A FMEDA was performed on this component during the development activities. This technique is an extension of the traditional failure mode and effect analysis (FMEA) in that it identifies online diagnostics techniques in the context of each failure mode analyzed. The conclusions of the FMEDA were verified using fault injection testing. The results of this analysis were used to reinforce weak aspects of the original design, and were also used to aid in the calculation of the various types of failure rates.

This criterion is another that represents a clear difference between IEC 61508 certified components and typical commercial components. There are certainly many other hazard analysis techniques that could be utilized but what has been done already is a very good start towards supporting the safe operation of the overall system.

The seventh criterion is common cause failure prevention, another subtopic of preventing systematic faults. The scope of this criterion is very limited at the component level and is simply focused on the documentation and availability of the design details of the component. Those details have been well documented and would be available as inputs to a system level assessment.

The eighth criterion is environmental qualification, the final subtopic of preventing systematic faults. The STZ Transmitter carries the CE Mark and FM Approval. From those certifications and from the operating parameters provided in the User's Manual, conclusions can be drawn about the component being adequate to perform normally in various environments, including explosive environments. The difficult aspect of this criterion is that environmental parameters can be very extreme in some applications, making it difficult to encompass all applications with these generic qualifications. While this component's level of qualification may be adequate for many environments, it can be expected that there will be some that are outside the bounds of how it was designed. The most obvious example is harsh nuclear radiation environments. Digital electronics are typically more susceptible to degradation from nuclear radiation than typical mechanical and analog components, so additional effort could be expected to make the component suitable for these types of environments.

The ninth and final criterion is suitability evaluation of "off-the-shelf" equipment. Successful operating experience is typically an important aspect of these evaluations, and in this case, there is no such experience data available

since the product is new to the market. This should be able to be worked around though, due to the extensive attention that has been paid to preventing systematic failures and extending the predicted FIT rate. Also, because of the third party certification activities performed, in this case, by exida it is positive that this manufacturer is experienced with audits of their design and associated processes. It can be expected that the manufacturer will be open to additional industry specific audits and/or surveys.

Fisher Controls DVC6200 SIS Digital Valve Controller

The first criterion is classification scheme. In this case, the exida certificate[76] indicated that the Fisher Controls Digital Valve Controller is SIL 3 capable. Just like with the previous evaluation, once a clear link is determined between the industry classification scheme and the SILs, the translation will be quite smooth, and industries will be able to easily determine which components will have the adequate level of rigor required for their specific applications.

The second criterion is defense against random hardware failures. The failure rates of this item were also calculated in FITs. Since this item can be configured in multiple ways that significantly impact the probability of failure, failure rates for each configuration are provided on the exida certificate. Some of those rates have been included in Table 5.2, and, just like in the first evaluation, these values could then be fed into the system level reliability analysis (deterministic or probabilistic) to ensure adequate reliability is going to be achieved.

The third criterion is lifecycle processes and designing techniques. The exida assessment report confirms that the lifecycle activities were audited and found to be in compliance with the applicable requirements of IEC 61508. A functional safety management (FSM) plan was used to direct the activities, and Table 5.2 includes a list of the tasks and documents that were included. The activities and documentation identified are very sufficient to support the overall system lifecycle activities.

The fourth criterion is built-in safety features. Within the design of the DVC6200 valve controller is included fault detection, backward recovery, a time triggered architecture, and static resource allocation. The fault detection coverage was evaluated to be sufficient during the FMEDA. Similar to the first evaluation, this level of attention to developing a safe design at the component level will have a positive impact on efforts to design the overall system to function safely.

The fifth criterion is design analysis, verification, and validation. Table 5.2 includes the specifics of what techniques were utilized from this category of activities. The exida assessment report indicated that there was intentionality in picking specific activities from Appendix B of IEC 61508 Part 2 [15] in order to meet the SIL 3 level of rigor. This is a good example of how this document is used successfully implement standardization between the industries and the manufacturers, and it also shows how manufacturers are pushed to a higher

level of rigor in their efforts to develop components that can successfully achieve certification, which then allows for better design integrity to be achieved at the system level.

The sixth criterion is hazard analysis. Just like for the first component that was evaluated, a FMEDA was performed to ensure the design was reliable and that fault detection coverage was sufficient. Observing that this same type of activity was involved in both components being evaluated is a positive indicator of the consistent level of rigor that is driven through the use of the IEC 61508 standard. In the typical commercial world, Hazard analysis are generally considered as luxuries and not absolute necessities because they require additional time and money and the components can possibly function properly without them. The use of the IEC 61508 standard pushes these luxuries into standard practice, which is a significant advantage for the high risk industries we are focused on throughout this thesis.

The seventh criterion is common cause failure prevention. This section of this evaluation is very similar to the first evaluation. The design details have been well documented and would be available as inputs to a system level assessment.

The eighth criterion is environmental qualification. This section is also very similar to the first evaluation. This component has many of the same environmental qualifications as the component in the first evaluation, which is good, but the potential for some applications requiring additional effort to evaluate remains.

The ninth criterion is suitability evaluation of “off-the-shelf” equipment. Unlike the component in the first evaluation, this one does have evidence of a successful operating history. Additionally, it also has the positive aspects of documented evidence of attention to the prevention of systematic faults. This manufacturer also shares the positive aspect of being open to and experienced with audits. These factors make this component a good candidate to be put through this type of suitability evaluation.

The previous two evaluations both support the use of IEC 61508 as a vehicle of standardization by demonstrating that the designs and associated processes of these two different manufacturers are held up to a consistent and desirable level of rigor at the component level. The resulting groundwork is then in place to support a very successful set of activities at the system level.

Additional Notes in Support of Standardization

The awareness of wild variation in the design practices and documentation practices of equipment manufacturers [1], [28] causes there to be a significant level of uncertainty at the beginning of suitability evaluation efforts. The use of IEC 61508 and the third party certifiers removes substantial amounts of that uncertainty.

While the US Nuclear industry is not currently taking advantage of IEC 61508 the way the process industry is, there are examples of other international nuclear industries doing so. One such example is in the UK. The UK has

developed a software based tool for extracting critical information from equipment manufacturers in a manner that facilitates efficient and effective evaluations and that tool (called EMPHASIS) is built on many of the requirements of the IEC 61508 standard [79]. This example indicates that there is also potential for the US Nuclear industry to implement and benefit from this methodology for removing uncertainty, improving efficiency, and increasing effectiveness of suitability evaluations of off-the-shelf equipment.

CHAPTER SIX

CONCLUSION

Comparison of Industries

For the purpose of comparing different industries that involve the mitigation of significant risk through the implementation of instrumentation and controls equipment, the four identified categories (classification, defending against random failures, preventing systematic faults, and suitability evaluations) provide insight into understanding where the similarities and differences are related to the implementation of off the shelf equipment.

Regarding the topic of classification, similarities were observed in the general intent of scaling the level of rigor to the safety significance of the equipment. Each industry had their own variations for categorizing the importance of the equipment in terms of the risks intended to be mitigated, but they all could potentially utilize the IEC 61508 SILs for standardization with manufacturers at the component level.

Some differences were perceived within the topic of defending against random failures, but while the reliability concepts (deterministic versus probabilistic) appeared to be incompatible at the overall system level, there is still potential for coherence at the lower component level. Underneath the system level deterministic single failure criterion and the probabilistic modeling approach, there is potential for the utilization of the reliability targets that are inherent to the SILs. Additionally, despite the system level differences in evaluating and confirming reliability, the implementation of redundancy was still the common approach to achieve the reliability goals.

Many similarities were seen within the topic of the prevention of systematic faults. The use of lifecycle processes, the use of hardware and software design verification and validation, the use of hazard/failure analysis, and attention to preventing common cause failure were all observed to be universal. There was variation in the levels of implementation between the different industries but the basic elements were there. Those basics are more than enough to support the unification of these industries behind IEC 61508 with equipment manufacturers. There were acknowledged differences regarding the parameters and level of rigor applied to environmental qualification, but this is not a fatal flaw for the proposed methodology. Supplemental environmental testing and additional mitigating strategies are already implemented by the DOD and nuclear industries so that aspect would simply continue to be necessary.

The practice of suitability evaluations of off-the-shelf equipment is implemented to varying degrees by the different industries, but when they occur they share common building blocks to prove or disprove suitability.

The final conclusion in this area is that IEC 61508 has the potential to be a very useful vehicle of standardization at the component level (component refers to a typical piece of industrial equipment, such as a sensing element, a logic

solver, or a control element.). It can be a successful link between all of these industries and the relevant component manufacturers. There are significant differences between complete systems but not among individual components. Utilizing the similarities at the component level has the potential to lead to a mutually beneficial relationship for the industries and manufacturers. The industries will have a wider range of better components available to them, while the manufacturers will be able to easily reach a larger customer base.

Suitability Evaluations of Off-the-Shelf Equipment.

At this point in time, the standards and guides of the US DOD and nuclear industry indicate significant risk in taking on evaluations of off-the-shelf equipment [1], [2], [28], but it has been shown that this same level of concern is not warranted for equipment that has been certified to be compliant with IEC 61508 SIL 2 and above requirements. Manufacturers that are able to achieve a SIL 2, 3, or 4 certification can be assumed to have a complete and fully implemented quality assurance program, and are being intentional about defending against random failures and preventing systematic faults. These are assumptions that cannot be made about any commercial manufacturer in general. It is a win-win situation for high risk managing industries to seek out manufacturers that are offering relevant products with these types of certifications. This kind of effort is expected to have financial and technical benefits for all parties.

Future Work

In the future, it could be beneficial to extend the survey to other industries such as commercial aerospace, NASA, food and drug production, and medical device manufacturing. Due to time limitations, these industries were not able to be include in this work.

It would also be beneficial to take a deeper look at the IEC 61508 SIL 1-4 requirements and specifically link them to the various classification schemes such as IEC 61226 Category A, B, and C, IEEE RISC 1-4, and IEEE Class 1E. This will be a critical task for empowering the different industries to embed the IEC 61508 SILs into their standard practices and for the regulators of those industries to be able to understand and fully embrace this methodology of utilizing this standard between equipment users and producers.

LIST OF REFERENCES

[1] Joint Software Systems Safety Engineering Workgroup, *Joint Software Systems Safety Engineering Handbook*. 2010.
[2] Electric Power Research Institute, “TR-107339 Evaluating Commercial Digital Equipment for High Integrity Applications,” 1997.
[3] G. Johnson, “Nuclear Use of I&C Equipment Certified for Commercial Safety Use,” in *Opportunities and Challenges for Water Cooled Reactors in the 21st Century*, 2009.
[4] G. Johnson, “Comparison of IEC and IEEE standards for computer-based control systems important to safety,” in *2001 IEEE Nuclear Science Symposium Conference Record*, 2001, no. HCSS++, pp. 2474–2481.
[5] R. T. Wood, R. Belles, M. S. Centiner, D. E. Holcomb, K. Korsah, A. S. Loebl, G. T. Mays, M. D. Muhlheim, J. A. Mullens, W. P. Poore, A. L. Qualls, T. L. Wilson, and M. E. Waterman, *Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems*. US NRC, 2009.
[6] J. Lee and K. Kwon, “Comparison of the Software Safety Criteria between IEC and IEEE Standards for the Digital Instrumentation and Control System,” in *Transactions of the Korean Nuclear Society Autumn Meeting*, 2006, pp. 1–2.
[7] D. Herrmann, *Software Safety and Reliability*. IEEE Comput. Soc. Press, 1999.
[8] D. S. Herrmann, “A methodology for evaluating, comparing, and selecting software safety and reliability standards,” *IEEE Aerosp. Electron. Syst. Mag.*, vol. 11, no. 1, pp. 3–12, 1996.
[9] Y. Papadopoulos and J. A. McDermid, “The potential for a generic approach to certification of safety critical systems in the transportation sector,” *Reliab. Eng. Syst. Saf.*, vol. 63, no. 1, pp. 47–66, Jan. 1999.
[10] International Society of Automation, *ISA-84.00.01-2004 Part 3 (IEC 61511-1 Mod) Functional Safety : Safety Instrumented Systems for the Process Industry Sector- Guidance for the Determination of the Required Safety Integrity Levels -Informative*, vol. 3. 2004.
[11] Institute of Electrical and Electronics Engineers, *IEEE 603 Standard Criteria for Safety Systems for Nuclear Power Generating Stations*. 2009.
[12] International Atomic Energy Agency, *SSG-30 Safety Classification of Structures , Systems and Components in Nuclear Power Plants*. 2014.
[13] International Electrotechnical Commisson, *IEC 61226 Nuclear power plants- Instrumentation and control important to safety- Classification of instrumentation and control functions*, 3.0 ed. 2009.
[14] US Department of Defense, *MIL-STD-882E Standard Practice for System Safety*. 2012.
[15] International Electrotechnical Commisson, *IEC 61508 Functional Safety Part 2: Requirements for Electrical/Electronic/ Programmable Electronic Safety-Related Systems*, 1.0 ed. 2000.
[16] International Society of Automation, *ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod) Functional Safety : Safety Instrumented Systems for the Process*

Industry Sector - Framework, Definitions, System, Hardware and Software Requirements, vol. 1. 2004.
[17] Institute of Electrical and Electronics Engineers, *IEEE 7-4.3.2-2010 Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations*. 2010.
[18] Institute of Electrical and Electronics Engineers, *IEEE 379 Standard for Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems*. 2014.
[19] Institute of Electrical and Electronics Engineers, *IEEE 577 Standard Requirements for Reliability Analysis in the Design and Operation of Safety Systems for Nuclear Power Generating Stations*. 2012.
[20] Institute of Electrical and Electronics Engineers, *IEEE 352 Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems*. 2010.
[21] International Atomic Energy Agency, *SSR-2/1 Safety of nuclear power plants : Design*. 2012.
[22] International Electrotechnical Commisson, *IEC 61513 Nuclear power plants – Instrumentation and control important to safety – General requirements for systems*, 2.0 ed. 2011.
[23] International Electrotechnical Commisson, *IEC 60987 Nuclear power plants- Instrumentation and control important to safety- Hardware design requirements for computer-based systems*, 2.0 ed. 2007.
[24] International Electrotechnical Commisson, *IEC 61508 Functional Safety Part 3: Software Requirements*, 1.0 ed. 1998.
[25] International Electrotechnical Commisson, *IEC 60880 Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions*. 2006.
[26] International Electrotechnical Commisson, *IEC 62138 Nuclear power plants – Instrumentation and control important for safety – Software aspects for computer-based systems performing category B or C functions*, 1st ed. 2004.
[27] Electric Power Research Institute, “EPRI NP-5652 R1 Plant Engineering: Guideline for the Acceptance of Commercial-Grade Items in Nuclear Safety-Related Applications,” 2014.
[28] Electric Power Research Institute, “TR-106439 Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications.” 1996.
[29] Electric Power Research Institute, “1011710 Handbook for Evaluating Critical Digital Equipment and Systems.” 2006.
[30] International Electrotechnical Commisson, *IEC 62671 Nuclear power plants- Instrumentation and control important to safety- Selection and use of industrial digital devices of limited functionality*, 1.0 ed. 2013.
[31] P. Gruhn and H. Cheddie, *Safety Instrumented Systems: Design, Analysis*

and Justification, 2nd ed. International Society of Automation, 2006.
[32] International Electrotechnical Commisson, *IEC 61508 Functional Safety Part 1: General Requirements*, 1.0 ed. 1998.
[33] International Society of Automation, *ISA-84.00.01-2004 Part 2 (IEC 61511-1 Mod) Functional Safety : Safety Instrumented Systems for the Process Industry Sector- Guidelines for the Application of ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1Mod) - Informative*, vol. 2. 2004.
[34] "PLC - Oil and gas regulation in the United States: overview." [Online]. Available: http://us.practicallaw.com/9-525-1545?source=relatedcontent#a318287. [Accessed: 15-Jan-2016].
[35] International Electrotechnical Commisson, *IEC 61508 Functional Safety Part 4: Definitions and Abbreviations*, 1.0 ed. 1998.
[36] International Electrotechnical Commisson, *IEC 61508 Functional Safety Part 5: Examples of Methods for the Determination of Safety Integrity Levels*. 1998.
[37] International Electrotechnical Commisson, *IEC 61508 Functional Safety Part 6: Guidelines on the Application of IEC 61508-2 and IEC 61508-3*, 1.0 ed. 2000.
[38] International Electrotechnical Commisson, *IEC 61508 Functional Safety Part 7: Overview of Techniques and Measures*, 1.0 ed. 2000.
[39] "Safety Automation Equipment List - (SAEL) - IEC 61508 certified process industry equipment." [Online]. Available: http://www.exida.com/SAEL. [Accessed: 31-Jan-2016].
[40] International Atomic Energy Agency, "From Obninsk Beyond: Nuclear Power Conference Looks to Future," in *International Conference on Fifty Years of Nuclear Power - the Next Fifty Years*, 2004.
[41] International Atomic Energy Agency, "50 Years of Nuclear Energy," pp. 1–9, 2004.
[42] International Atomic Energy Agency, "Convention on Nuclear Safety (CNS)," 2014. [Online]. Available: http://www-ns.iaea.org/conventions/nuclear-safety.asp. [Accessed: 19-Dec-2015].
[43] International Electrotechnical Commisson, *IEC 60780 Nuclear power plants – Electrical equipment of the safety system – Qualification*, 2nd ed. 1998.
[44] International Electrotechnical Commisson, *IEC 60980 Recommended practices for seismic qualification of electrical equipment of the safety system for nuclear generating stations*. 1989.
[45] International Electrotechnical Commisson, *IEC 62003 Nuclear power plants – Instrumentation and control important to safety – Requirements for electromagnetic compatibility testing*, 1.0 ed. 2009.
[46] International Electrotechnical Commisson, *IEC 62645 Nuclear power plants – Instrumentation and control systems – Requirements for security programmes for computer-based systems*, 1.0 ed., vol. 2002. 2014.
[47] US Nuclear Regulatory Commission, *NUREG-1650, Rev 5, The United*

States of America National Report for the Convention on Nuclear Safety. 2013.
[48] US Nuclear Regulatory Commission, *10 CFR Part 50—Domestic Licensing of Production and Utilization Facilities*. .
[49] US Nuclear Regulatory Commission, *10 CFR Part 52—Licenses, Certifications, and Approvals for Nuclear Power Plants*. .
[50] S. Burns, "Looking Backward, Moving Forward: Licensing New Reactors in the United States," *Nucl. Law Bull.*, no. 81, pp. 7–29, 2008.
[51] US Nuclear Regulatory Commission, *10 CFR Appendix B to Part 50—Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants*. .
[52] American Society of Mechanical Engineers, *ASME NQA-1-2012 Quality Assurance Requirements for Nuclear Facility Application*. 2012.
[53] US Nuclear Regulatory Commission, *10 CFR Part 21—Reporting of Defects and Noncompliance*. .
[54] US Nuclear Regulatory Commission, *Regulatory Guide 1.152, Rev. 3, Criteria for Use of Computers in Safety Systems of Nuclear Power Plants*. 2011.
[55] Institute of Electrical and Electronics Engineers, *IEEE 323 Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations*. 2003.
[56] "NPEC Standards." [Online]. Available: http://grouper.ieee.org/groups/npec/npec-standards.html. [Accessed: 03-Jan-2016].
[57] Institute of Electrical and Electronics Engineers, *IEEE 344 Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations*. 2004.
[58] French Nuclear Safety Authority, *Sixth French Report under the Convention on Nuclear Safety*. 2013.
[59] "IEC I&C Standards in the nuclear sector | IEC e-tech | August 2013." [Online]. Available: http://iecetech.org/issue/2013-08/IEC-I-C-Standards-in-the-nuclear-sector. [Accessed: 05-Jan-2016].
[60] Department of Energy & Climate Change, *The United Kingdom's Sixth National Report on Compliance with the Convention on Nuclear Safety Obligations*. 2013.
[61] "Energy Act - GOV.UK." [Online]. Available: https://www.gov.uk/government/collections/energy-act. [Accessed: 06-Jan-2016].
[62] Kingdom of Belgium, Germany, Spain, United Kingdom, Sweden, and Finland, "Licensing of safety critical software for nuclear reactors," 2013.
[63] "About Department of Defense." [Online]. Available: http://www.defense.gov/About-DoD. [Accessed: 09-Jan-2016].
[64] International Atomic Energy Agency, "NP-T-3.12 Core Knowledge on Instrumentation and Control Systems in Nuclear Power Plants," 2011.

[Online]. Available: http://www-pub.iaea.org/books/IAEABooks/8490/Core-Knowledge-on-Instrumentation-and-Control-Systems-in-Nuclear-Power-Plants. [Accessed: 06-Feb-2016].
[65] A. Coppola, “Reliability Engineering of Electronic Equipment: A Historical Perspective,” *IEEE Trans. Reliab.*, 1984.
[66] R. E. Barlow, “Mathmatical Theory of Reliability: A Historical Perspective,” *IEEE Trans. Reliab.*, 1984.
[67] International Atomic Energy Agency, *NS-G-1.3 Instrumentation and Control Systems Important to Safety in Nuclear Power Plants*. 2002.
[68] NRC, “Use of Probabilistic Risk Assessment Methods in Nuclear Activities: Final Policy Statement,” *60 Fr 42622*. 1995.
[69] W. Goble, *Control Systems Safety Evaluation and Reliability*, 3rd ed. International Society of Automation, 2010.
[70] Institute of Electrical and Electronics Engineers, *IEEE 1012-2012 Standard for System and Software Verification and Validation IEEE Computer Society*, vol. 2012, no. May. 2012.
[71] R. Torok, B. Geddes, M. Bailey, L. Friel, J. Thomas, B. Antoine, N. Geddes, D. Blanchard, and N. Thuy, “Hazard Analysis Methods for Digital Instrumentation and Control Systems,” 2013.
[72] R. T. Wood, *Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems*. 2008.
[73] exida, “MII STZ Dual Sensor Transmitter Certificate,” 2015.
[74] exida and D. Butler, “Results of the IEC 61508 Functional Safety Assessment for the MII STZ Dual Sensor Transmitter,” 2015.
[75] Moore Industries International, “STZ User’s Manual,” 2016.
[76] exida, “Fisher Controls DVC6200 SIS Digital Valve Controller Certificate,” 2013.
[77] exida, D. Butler, and I. van Beurden, “IEC 61508 Functional Safety Assessment of the DVC6200 SIS Digital Valve Controller and Position Monitor,” 2013.
[78] Fisher Controls, “FIELDVUE ™ DVC6200p Digital Valve Controller Instruction Manual,” 2015.
[79] T. S. Lockhart, “Vetting Smart Instruments for the Nuclear Industry,” 2015. [Online]. Available: http://www.miinet.com/Portals/0/PDFs/Vetting_Smart_Instruments_for_the_Nuclear_Industry_White_Paper_Moore_Industries.pdf. [Accessed: 01-Feb-2016].

VITA

Andrew Michael Nack graduated from the University of Missouri-Columbia in 2006, with a Bachelor of Science in Electrical Engineering. His first job after college was at Y12 National Security Complex in Oak Ridge, TN where he was a Cat. 2 Facility Instrumentation and Controls Design Engineer. In that role, he designed the instrumentation and controls for new equipment and developed design changes to existing equipment that was used in DOE classified applications. This initial position was mainly made possible because he worked as an intern at the DOE facility in Kansas City, MO (the Kansas City Plant, managed by Honeywell) in the summer between his junior and senior years of college.

In the fall of 2008, he took a job as an Equipment Qualification Engineer at ATC Nuclear (known at the time as Southern Testing Services), originally based in Knoxville, TN and is now located in Oak Ridge, TN. There he learned the art of commercial grade dedication in the context of the US commercial nuclear power generation industry. He also learned and became proficient at designing and supervising various environmental qualification tests such as seismic, radiation, and electromagnetic compatibility for various types of equipment used in commercial nuclear power safety applications.

In January of 2012 he became a licensed professional engineer in the state of TN after passing the electrical engineering PE exam.

While working for ATC, he also was able to get involved with the EPRI nuclear working group on electromagnetic compatibility, and also joined Sub-Committee 6 (Safety Systems) of the IEEE Nuclear Power Engineering Committee. Through these groups, he was able to be involved in work developing revision 4 of EPRI TR-102323, the 2016 version of IEEE 7-4.3.2, and a new standard IEEE P1891. He is also a corresponding member of ISA Sub-Committee 67 which deals with topics related to nuclear instrumentation and controls.

Then in December of 2012, he was promoted to Senior Instrumentation and Controls Engineer and Principal Engineer of the ATC Nuclear TN office. In this role he continued to be involved in some of the same equipment qualification activities but moved into dealing with more digital equipment instead of the analog and mechanical components he originally dealt with. It was this change that motivated him to pursue his Master of Science in Computer Engineering at the University of Tennessee-Knoxville and for him to pursue this particular thesis topic.