Successful compliance with IEC 61508 safety standards

Irv Badr
Patchanee Petprayoon

The international standard, IEC 61508, provides guidelines for developing systems that comprise electrical, electronic, or programmable electronic components, or a combination of those components that perform safety functions. This article offers techniques for incorporating those guidelines into the embedded system and software development lifecycle. It also provides examples of use cases to apply software and system engineering methods and a strategy to help enhance the reliability and functionality of the safety-related and safety-critical systems.

Introduction

Computer-based systems, or programmable electronic systems (PESs), are increasingly required in all industries to comply with safety standards. Traditionally, this has not been the trend, because systems previously comprised mostly electrical or electronic components, not PESs. Those components were commonly earmarked for safety compliance rather than for the complete system. However, with increased use of software-based control and communications systems, safety standards have been expanded to incorporate this new development in systems engineering.

The International Electrotechnical Commission standard, IEC 61508, titled Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES), describes a generic approach for all safety activities for systems that are used for safety functions. In most situations, safety is achieved by several protective systems that rely on various technologies. Therefore, any safety strategy must take into consideration not only all of the elements within an individual system (for example, sensors, controlling devices, and actuators) but also all of the safety-related systems. It can also provide a framework for considering safety-related systems dependent on other technologies.

This article offers a roadmap for adoption of the IEC 61508 guidelines and techniques for incorporating them into the system and embedded software development lifecycle. It also provides examples of use cases to apply software and system engineering methods and a strategy to help enhance the reliability and functionality of the safety-related and safety-critical systems.
By using a cross-functional approach and tools, you can better manage and incorporate the IEC 61508 guidelines into your product development process. This not only helps ensure product safety but also helps increase system reliability and minimizes the hazardous and risk-escalating incidents that can have a severe impact on human life and the environment.

**Compliance challenges**

- Growing compliance issues, involving safety, security, and environmental protection
- Safety and reliability compliance efforts are manually intensive and time-consuming, which makes it very difficult to establish, maintain, and demonstrate compliance with various standards and regulatory bodies
- Ongoing challenges and higher than necessary costs in getting the product certified by different agencies due to the inability to effectively find and link critical information during the certification process
- Lack of integration and visibility between processes, tools, and data causing the disjointed disciplines, making it difficult to trace and identify the impact of changes in safety-related or safety-critical systems
- Lack of documented policies and procedures and insufficient traceability from requirements to: design, development, testing, and change management.
- Also, the impact of a process that involves failing critical equipment, which could be life-threatening or endanger public safety or the environment, needs to be part of traceability. This is known as *impact analysis*.

**Why safety and safety-critical systems certification is critical for manufacturers**

From a manufacturer’s perspective, safety-related certification of a critical system to comply with an international standard, such as International Electrotechnical Commission (IEC 61508), greatly enhances the credibility of their product. When bidding on a project, it is common for buyers to specify mandatory compliance with IEC 61508 by manufacturers and suppliers. The higher system integrity level (SIL) that suppliers can demonstrate to buyers, the greater their competitive advantages and the better their chances of winning the contract.

High-quality architecture to ensure public safety is essential to the success of these safety-related or safety-critical systems. For example, if the sensors or actuator inside the underlying devices in a system fail, the incident should have minimal impact on human and environmental safety for vendors and manufacturers to release an IEC 61508-certified system. Suppliers are required to demonstrate, through traceability, every step of the systems and software development processes and show that they have an adequate process to document, implement, and track safety requirements.

So the big question might be: Do we have enough justification to adopt this suggested automation that improves efficiency and, at the same time, improves safety compliance? In other words, is the return on investment (ROI) sufficient? The answer is: IEC 61508 certification. It gives both hardware and software vendors significant advantages over their competitors, among other benefits, and more than justifies the investments of time and money.
Overview of an effective approach

Collaborative Lifecycle Management applications

Rational Method Composer integrates with applications that comprise the Rational solution for Collaborative Lifecycle Management (CLM), such as IBM® Rational Team Concert™. By taking advantage of these integrations, the process engineering, product development, and project delivery teams can be sure that the different engineering teams are following correct and consistent practices. CLM provides continuity in workflow through linking configuration and change management, requirements management, and testing into a single solution. To varying degrees, the utility provided by CLM is universally applicable to all team-based projects.

The approach that we describe in this article is applicable across various industries where development of safety and reliability of the system are critical, such as industrial process control, oil and gas, chemical and petroleum, mining, and nuclear plant. The usage patterns explore the interaction between process engineer and the development teams that have access to the organization’s project development process guidelines, data, workflows, and collaboration tools. It shows how requirement management tools such as IBM® Rational® DOORS® and Rational Requirements Composer can effectively manage requirements across the project’s lifecycle and how IBM® Rational Team Concert™ can help teams of engineers that are geographically dispersed improve their processes. This increases control over software and system development discipline to avoid risks and lower the cost and complexity of the projects.

Planning

Guiding business goals and requirements according to regulatory standards, such as the seven parts of IEC 61508, enables safety planning to propagate into development and implementation layers of the organization.

Figure 1. High-level overview of this combination

---

Successful compliance with IEC 61508 safety standards
Processes and tools

Consequently, you need a tool and process that help in quickly identifying the impact of changes in the requirements and trace the relationship to various components, subcomponent, and system. The emphasis here is on the delivery process. Given that change is unavoidable, when changes happen, the product delivery team's flexibility and adaptability to adjust to these changes is vital to success.

Successful product development starts with modern requirements management software

We must capture, analyze, and manage requirements from concept to the end of the project lifecycle. Requirements management software, such as Rational Requirements Composer, helps manage unmanageable data across the business units and domains.

The development of highly safe and reliable devices and systems depends greatly on the collaboration of the many individuals and teams involved in the engineering processes. For the system vendors to reduce the hazard, risk, and complexity of the project, it is critical for the organization to have robust requirements management software that enable engineers to effectively manage requirements and avoid scope creep (in stakeholder requirements, customer requirements, regulatory requirements, safety requirements, functional requirements, nonfunctional requirements, design requirements, safety requirements, and so forth). This not only enables the organization to better respond to requirement changes but also helps with other key factors:

- Better risk management
- Ensuring product quality, reliability, and safety
- Timely execution of the project plan
- Traceability across the product lifecycle
- Elimination of rework
- Faster time to verify, validate, and test the product
- Shorter time to market

Building a safe, secure, reliable product is a team effort. It requires constant collaboration among the multiple teams and stakeholders. The perception of safety by a system safety specialist might be completely different from that of a software engineer. Automated requirements management tools and workflow allow geographically dispersed engineering teams to collaborate on the same project concurrently. This enables the teams to identify, verify, and remove any unclear or toxic requirements that should not be included in the system design.

Identify the initial requirements for the overall safety lifecycle, and break down those complex requirements into the smaller, easier to manage chunks of requirements.

In the flow diagram in Figure 2, there are numerous differentiated steps between the top-level concept, or definition of safety, and its subsequent implementation and validation. These steps are covered in IEC 61508 Part 1.
Successful compliance with IEC 61508 safety standards

**Figure 2. Safety lifecycle (source IEC 61508 Part 1)**


To simplify the management of standards related requirements, it's best if we use the actual IEC 61508 standard as the starting point for developing standards related requirements. Development of requirements involves analysis and interpretation, which is best performed by a team of domain experts who undertake the job of reviewing and identifying these requirements.

The safety lifecycle diagram in Figure 2, which was captured in IBM® Rational® Method Composer, helps us identify the initial requirements for the overall safety lifecycle. This makes it easier for the process engineer to capture and break down those complex requirements into the small manageable segments to follow the lifecycle.

In a complex, multiyear project, it is customary to spend several months in gathering and analyzing initial requirements before actual design work can proceed. As much as we want to control and keep the design requirements consistent throughout the course of the project, that is a challenging goal. Often, external forces, such as influential stakeholders, force requirements to change (for example, new regulations, new standards, or new legal requirements). This greatly contributes to cost overrun and delays in the product delivery schedule.
IBM Rational Method Composer for process authoring

Rather than painstakingly digging through a stack of paper searching for the right process to follow, it's better to automate the task so that similar process steps can be viewed instantaneously. We use Rational Method Composer because of the flexibility and the adaptability of its underlying tools. We use it to publish our system and software engineering processes, guidelines, best practices, and methodology in HTML format on the web server, or an internal file server, as opposed to paper binders.

Development processes that need changes can be quickly adapted, modified, or extended by process engineers and made available to the rest of the team quickly. Traceability is essential to compliance. Therefore, having your organization's processes documented in one place, where traceability can be quickly established, proves to be very effective in streamlining workflow and during audits.

Through a tightly integrated process and the combination of Rational Method Composer and, for change management, IBM® Rational Team Concert™, the various processes and best practices that we captured in the methods tool can be exported and shared among teams and projects. Doing so enables members of various engineering disciplines to collaborate and share their best practices and methods. That encourages reuse within the organization to help increase the product quality and meet the regulatory standards and guidelines.

As an example, software written according to IEC 61508 Part 3, the IEC 61508 standard recommends following a V-model development process. As Figure 3 shows, we must reveal the relationship between the requirements for system design, software safety, architecture, design, and code to software module testing, integration, and validation throughout the entire development process, all the way through system-wide safety validation.

Safety is relevant all levels of the systems delivery process. Rational Method Composer enables the delivery team to explicitly define and enforce safety in the V model, which is a prevailing best practice in workflow.

Figure 3. A V-model development process diagram captured Rational Method Composer

According to the V-model development process, the software module testing must ensure that the software is fully tested at the functional-level development. All of the software development tasks and activities to be carried out to develop the safety-related software are captured and defined...
within Rational Method Composer. The development process takes a top-down approach based upon these stages:

- Software safety requirement specifications
- Architectural, component, and module design
- Testing and software integration
- Verifying and validating up to the point where the hardware and software integration occurs

A key benefit of including the IEC 61508 guidelines and following the V-model development process is realized by means of acceptance tests and other activities defined in the quality and safety plan for the project. With a clearly defined processes, tasks, and activities, you can be confident and ready to prove to auditors that those devices and systems are developed based on best practices and safety and reliability standards. For the process engineer, we suggest that you thoroughly evaluate your organization's software development process and then review and extend them accordingly. How you would like to implement and interpret them is up to you, of course.

At the end of the day, the majority of the decisions still depend upon the vendors — how they selectively interpret the requirements and how much of the requirements from the standard are applicable to them.

Obviously, the higher the system integrity levels that the vendors are trying to achieve, the more stringent the techniques and requirements are that need to be implemented. The device or systems with lower SILs (such as SIL1 and SIL2) are less expensive for the vendors to implement. The higher SILs (such as SIL 3 and SIL 4) require a lot more money and time. Therefore, it will require a more substantial effort to validate and revalidate the systems, which ultimately lead to a higher cost of training of operators.

In short, the Rational solution for Collaborative Lifecycle Management (CLM), described previously, proves to be vital for synchronizing changes across the business domains and the supply chain. You can improve efficiency by using the well-established process template to streamline work from business units. This provides an integrated approach for the entire ecosystem.

Summary

For system vendors to reduce hazard, risk, and complexity of a project, it is critical for the organization to implement a requirements-centric workflow to manage requirements effectively, particularly safety- and security-related requirements. Process authoring based on system and software engineering best practices helps companies comply the various standards. By using the technology, tools, and processes described in this article, organizations can easily adopt and apply various safety standards, such as IEC 61508, and incorporate these into the development lifecycle.

All of the capabilities and functionality mentioned in this article can be implemented effectively with what the software includes. You can then easily customize and extend the application or tools to fit your organization’s needs.
Through a systematic approach, you can increase the efficiency of geographically distributed teams, so they can collaborate through interactive use of change, configuration, and project management software. This makes it faster to solve any problem.

For the system vendors and system integrator, the higher the system integrity level (SIL) that they can demonstrate to the buyer, the more competitive advantages they gain, which helps increase their chance of being the selected vendors or supplier for the projects.

Therefore, for the system and software development organization, the Rational solution for Collaboration Lifecycle Management (CLM) not only helps improve the quality of development processes but also helps reduce the risk and manage the delivery of complex systems and software.

**Appendix: More about concepts in this article**

This approach helps simplify the complex delivery process for systems and software by breaking the compliance process and requirements into manageable pieces and distributing them among the various teams.

**Where and when to start**

Incorporating the safety requirements into the product design requirements at the coding phase has proven not to be effective enough to demonstrate the safety and security of the products. Building a safe and secure product requires that organizations have well-defined processes and methods for planning, designing, developing, testing, implementing, and decommissioning.

Therefore, we cannot afford to incorporate the safety, security, and compliance requirements at product release time. Regulatory, safety, functional, nonfunctional, and stakeholder requirements need to be captured, evaluated, and planned for from the beginning of your product development.

Tracing information from the requirements all the way to the test case and the test result helps the testing team quickly identify the root cause of the problem and alert the interested person in the timely manner.

The question here is: How can we help all of the vendors provide integrated control of their safety functions to help advance their product safety and functionality, without compromising safety?

**Key steps for a strategy to implement the IEC 61508 standard**

1. Decide which standards, guidelines, and subcomponents of those standards to address.
2. Define your organization's goals and strategies for how to achieve that standard, before implementing those plans.
3. Develop a strategy for how you want to implement the IEC 61508 standard and apply them into your systems and software development lifecycle processes

Use robust requirements management tools to manage requirements throughout the product lifecycle and avoid scope creep. The software should help you:
- Build an understanding among team members of the applicable requirements, guides, and other documents.
- Identify initial requirements and traceability relationships, including relationships such as "consists of," "verifies," "tested by," "implemented by," and so forth.
- Enforce the policies and procedures that your organization adopted. Traceability must be enforced to ensure consistency, completeness, and traceability of your requirements.

Traceability from requirements through project development to testing and delivery enables organizations to accomplish critical things:

- Know which requirements are implemented and tested and which are not
- Collaborate and identify the impact of changes across the project's lifecycle
Related topics

• For more information related to the standards mentioned in this article:
  • IEC 61508 standard edition 2010
  • Learn more about Rational Method Composer:
    • Check the Rational Method Composer overview, page, where you can also download it for a free trial.
    • To learn about using Rational Method Composer with Jazz, including FAQs, links to enablement materials, and tips and tricks, see the Rational Method Composer and Practices wiki on developerWorks.
  • Find out more about Rational Team Concert:
    • Check the product overview page.
    • Check the Rational Team Concert page on Jazz.net.
    • Watch the Using Rational Team Concert in a globally distributed team webcast or a demonstration of the Dashboards and reports.
  • Browse the Rational DOORS Next Generation page on Jazz.net. For detailed instructions, explore the Rational DOORS Information Center.
  • You can find more information about the Rational solution for Collaborative Lifecycle Management on the CLM page on Jazz.net.
  • Subscribe to a developerWorks newsletter.
  • Get the free trial download for Rational DOORS Web Access.
  • Evaluate IBM software.