PERFORCE

WHITE PAPER

Achieving IEC 61508 Compliance

Introduction

Safety-critical companies can quickly and cost-effectively prove compliance with the IEC 61508 standard by using an integrated product development management solution.

The increased use of software-based control systems has led to an expansion of safety standards in a number of industries. Most of these standards are based on the broad IEC 61508 standard created by the International Electrotechnical Commission (IEC). Titled "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems," IEC 61508 is the international standard that covers functional safety in devices and machinery that use software-based or similar electronic safety-related systems to reduce risk to an acceptable level.

This solution brief details how Perforce Software's product development management solutions help companies achieve compliance with IEC 61508.

New Challenges in Functional Safety

Advancing technologies and increasing product complexities in the automotive, aerospace, and other safety-critical markets are bringing new challenges to product developers as they work to ensure the safety and security of their products. Functional safety is becoming stricter and more widespread in markets such as medical device manufacturing, the railway industry, and even solar energy. Safety-related systems in these markets must operate dependably, sometimes in demanding environments.

These safety functions are increasingly carried out by electric, electronic, and programmable safety-related systems. IEC 61508 contains requirements intended to prevent dangerous failures or, if they occur, minimize any harm a failure might cause.

Designing safety systems while meeting the latest functional safety requirements can be a challenging job for product developers. Adding to the challenge is the increased complexity software brings to the product development cycle and the pressure of beating competitors to market.

To meet these challenges, many companies adopt integrated, end-to-end product development management solutions. These solutions track all artifacts and work items associated with the development process and automatically generate the reports and traceability matrices necessary to prove compliance with functional safety regulations such as IEC 61508.

To better understand the benefits of a product development solution, let's start with a high-level overview of IEC 61508. Then we'll look at Perforce's product development solutions to see how they help teams meet the requirements and challenges the standard presents.

PERFORCE SOFTWARE'S FUNCTIONAL SAFETY FEATURES

Perforce's comprehensive and flexible solutions reduce project risk, improve visibility into project status, and increase team collaboration and communication via:

- Requirements management, impact analysis, and traceability
- Task and issue management
- Audit logging and electronic signatures
- Process automation and enforcement
- Centralized, secure storage of intellectual property
- Role-based security
- Metrics and reporting for management
- Support for any development process (Agile, Waterfall, etc.)

Designing safety systems while meeting the latest functional safety requirements can be a challenging job for product developers. Adding to the challenge is the increased complexity software brings to the product development cycle and the pressure of beating competitors to market.

An Overview of IEC 61508

IEC 61508 centers on the concepts of risk and safety functions. It defines risk as a function of the frequency or likelihood of a hazardous event occurring, as well as the severity of the consequences of an occurrence. An identified risk is reduced to a tolerable level by applying safety functions, which may consist of Electrical/Electronic/Programmable Electronic (E/E/PE) safety-related systems or other technologies. While other technologies may be employed in reducing the risk, only those safety functions relying on E/E/PEs are covered by the detailed requirements of IEC 61508.

Two types of general requirements are deemed necessary by the standard to achieve functional safety:

- Safety function requirements: What the function does.
- Safety integrity requirements: The likelihood of a safety function being performed satisfactorily.

The safety function requirements are derived from a hazard analysis, while the safety integrity requirements come from a risk assessment.

HAZARD ANALYSIS AND RISK ASSESSMENT

According to IEC 61508, zero risk can never be attained; there will always be some likelihood of a hazardous event occurring. Therefore, safety must be considered from the beginning of the development process, and nontolerable risks must be reduced to "as low as reasonably possible" (ALARP).

To identify potential hazards, the standard requires product development teams to perform a hazard analysis and risk assessments of equipment under control (EUC). For each hazard identified, the level of risk must be evaluated or estimated.

The standard does not mandate a specific method for determining the safety integration levels (SILs), saying only "either qualitative or quantitative hazard and risk analysis techniques may be used," and offering guidance on a number of approaches.

IEC 61508 PARTS

The standard is comprised of seven parts. The first three contain the requirements of the standard, while the remainder spell out the guidelines and provide examples for development.

It also includes Part 0, which is an introductory section titled "Functional Safety and IEC 61508." This section provides background information that helps users understand the rest of the standard.

IEC 61508 PARTS	SUMMARY
Part 1	General requirements
Part 2	Requirements for E/E/EP safety-related systems
Part 3	Software requirements
Part 4	Definitions and abbreviations
Part 5	Examples of methods for the determination of safety integrity levels
Part 6	Guidelines on the application of Parts 2 and 3
Part 7	Overview of techniques and measures

WHAT IS "FUNCTIONAL SAFETY"?

IEC 61508 defines "functional safety" as part of the overall safety of the equipment under control (EUC) and the EUC control system. Functional safety depends on the correct functioning of the E/E/PE safety-related systems.

For example, a thermal sensor in an electric motor that tells the control system to shut the motor down before it can overheat is an instance of functional safety. However, specialized insulation designed to protect the motor from high exterior temperatures is not an instance of functional safety, although it is still an instance of safety and could protect against the same hazard.

The functional safety standard IEC 61508 is applied to ensure that electronic systems are acceptably safe. It defines four general Safety Integrity Levels (SILs) with SIL 4 denoting the most stringent safety level. Each level represents an order of magnitude of risk reduction. The higher the SIL level, the greater the impact of a failure and the lower the failure rate that is acceptable.

Safety Integrity Level is a way to indicate the tolerable failure rate of a particular safety function. IEC 61508 requires the assignment of a target SIL for any E/E/PE safety-related system.

BASIS FOR OTHER STANDARDS

IEC 61508 has been used as the basis for the following sector-specific standards for functional safety:

- ISO 26262 for automotive electric/ electronic systems
- IEC 62279 for railway applications
- IEC 61511 for manufacturing processes
- IEC 61513 for nuclear power plants
- IEC 62061 for machinery system design
- IEC 62304 for medical devices

Perforce Helps Prove Compliance

Perforce's integrated product development management solutions, which include Helix ALM and Surround SCM, offer significant productivity and cost benefits for companies that must comply with the IEC 61508 standard or its derivatives for specific industries. Together, Helix ALM and Surround SCM make compliance verification easier, less error prone, and more cost effective by automating the creation, management, maintenance, and documentation of requirements traceability.

The requirements for software configuration management are outlined in IEC 61508-3, section 6.2.3. How Perforce's solutions help meet the standard's requirements for software configuration management are outlined in Table 1.

Perforce's integrated product development management solutions offer significant productivity and cost benefits for companies that must comply with the IEC 61508 standard or its derivatives for specific industries.

IEC 61508-3 6.2.3	Perforce
A) Apply administrative and technical controls throughout the software safety lifecycle, in order to manage software changes and thus ensure that the specified requirements for safety-related software continue to be satisfied;	✓
B) Guarantee that all necessary operations have been carried out to demonstrate that the required software systematic capability has been achieved;	✓
C) Maintain accurately and with unique identification all configuration items which are necessary to meet the safety integrity requirements of the E/E/PE safety-related system. Configuration items include at least the following: safety analysis and requirements; software specification and design documents; software source code modules; test plans and results; verification documents; pre-existing software elements and packages which are to be incorporated into the E/E/PE safety-related system; all tools and development environments which are used to create or test, or carry out any action on, the software of the E/E/PE safety-related system;	✓
D) Apply change-control procedures: • To prevent unauthorized modifications; to document modification requests; • To analyze the impact of a proposed modification, and to approve or reject the request; • To document the details of, and the authorization for, all approved modifications; • To establish configuration baseline at appropriate points in the software development, and to document the (partial) integration testing of the baseline; • To guarantee the composition of, and the building of, all software baselines (including the rebuilding of earlier baselines).	✓
E) Ensure that appropriate methods are implemented to load valid software elements and data correctly into the run-time system;	✓
F) Document the following information to permit a subsequent functional safety audit: configuration status, release status, the justification (taking account of the impact analysis) for and approval of all modifications, and the details of the modification;	✓
G) Formally document the release of safety-related software. Master copies of the software and all associated documentation and version of data in service shall be kept to permit maintenance and modification throughout the operational lifetime of the released software.	✓

Table 1: Perforce helps meet all the requirements for software configuration management under IEC 61508-3.

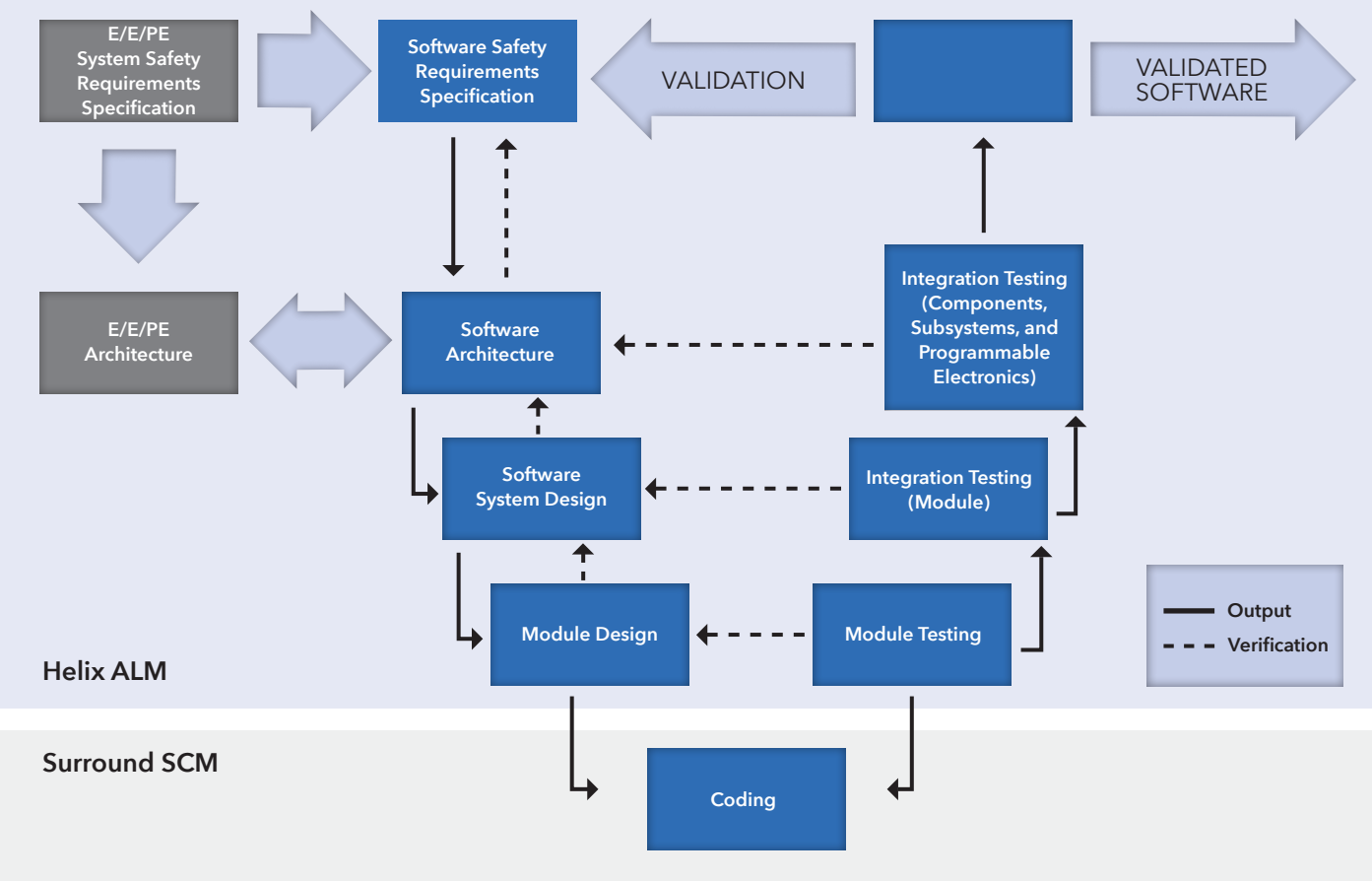

Figure 1: Perforce covers the entire software systematic capability and the development lifecycle V-model, from IEC-61508-3

With Helix ALM managing all product development and testing artifacts and Surround SCM managing the code, Perforce offers a tightly integrated solution that spans the entire development lifecycle described in IEC 61508-3 (see Figure 1).

Perforce Product Development Management Solutions

Designed for the most demanding product development environments, Perforce's product development lifecycle management solutions are scalable, feature-rich, team-based solutions for requirements management, test planning and management, issue tracking, software configuration management, and automated software testing. Our solutions seamlessly integrate these processes to provide end-to-end traceability of artifacts and more efficient control of product development.

REQUIREMENTS MANAGEMENT

Helix ALM manages the complete requirement lifecycle including planning, specification, review, validation, change management, and reporting. It also facilitates collaboration, automates traceability, and helps satisfy compliance with IEC 61508.

Helix ALM centralizes requirements management and keeps all stakeholders informed of new and changed requirements, makes participating in the review process easy, and ensures they understand the impact changes will have on a project.

Requirements can be organized into requirement documents, and users can easily structure document hierarchies and share common requirements between documents for improved reusability.

TRACK EVERYTHING THAT DEFINES A REQUIREMENT WITH HELIX ALM

- Details, description, images, etc.
- Review notes, conversations, and questions
- Change history, workflow, etc.
- Baselines and versioning
- Links to related artifacts including risk, tests, etc.

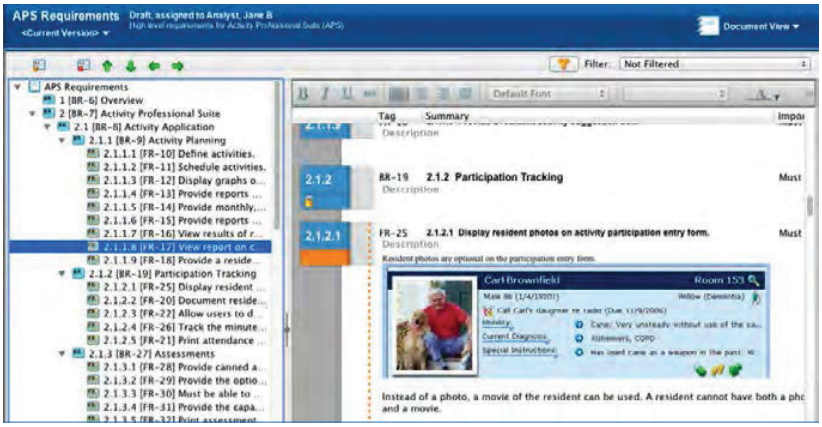

Figure 2: Requirements can be grouped into documents.

TEST MANAGEMENT

Testing complex products requires thousands of unique test cases, the time to execute them, and the ability to efficiently track and manage results. Helix ALM provides a complete solution to create, organize, execute, measure, and report on manual and automated testing efforts.

Helix ALM's centralized test management helps the team work together to create, organize, run thousands of test cases, track results, and measure progress.

Helix ALM simplifies managing large numbers of test cases and results by grouping them into test sets for better organization and reporting. For example, all tests for alpha testing can be included in one test set, and all tests for beta testing can be included in a separate set.

RISK MANAGEMENT

While risk can be managed with documents or spreadsheets, Helix ALM makes risk analysis and mitigation processes faster and easier by automating traceability matrices and risk reports. Users can easily conduct risk analyses (such as FMEAs) and continually monitor and enforce risk mitigation measures as the product moves through the development cycle.

Figure 3: Helix ALM can quickly generate FMEA reports.

To enable reuse of repetitive test steps, users can share test case steps with other test cases. Helix ALM can also automatically create test cases by intelligently recording a user's actions during manual or exploratory testing. With Helix ALM running in the background, the user builds a detailed history of the test session, which can be saved as a step-by-step test case for future reuse.

TRACK ALL TESTING ARTIFACTS WITH HELIX ALM

- Test case details
- Test steps
- Variants
- Test runs
- Workflow
- Email conversations
- Links to requirements and issues

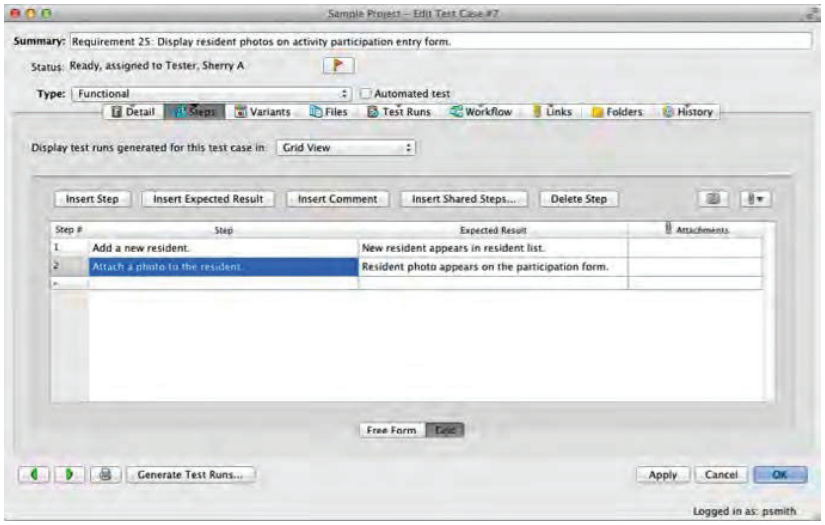

Figure 4: Helix ALM enables users to create reusable test case steps that can be shared with other test cases.

ISSUE MANAGEMENT

Helix ALM provides centralized management of issues, feature requests, and other tasks. This keeps the team in sync regarding outstanding issues, enables analysis and investigation of recurring problems, and allows tracing issues back to their source.

Work item information is included in the traceability matrix to provide a foundation for a ensuring product quality. In addition, the team can use this data to strengthen risk analysis and mitigation activities. It becomes much easier to find the root cause of issues, for example, and take corrective action when issues and requirements are linked.

Helix ALM's built-in reports help teams evaluate overall product quality levels and ensure risk mitigation strategies are working.

CHANGE MANAGEMENT

Change is constant in product development and often occurs at a blistering pace. Efficiently controlling and tracking change is critical to maintaining functional safety.

Surround SCM manages all changes to the product's digital assets (e.g., source code, database files, and graphics) and makes them available to the team anytime and anywhere.

Helix ALM's impact analysis reports make it easy to assess the impact of a requirement change before it is made. Users can perform an impact analysis to view the related items, assess the risk of making changes, and identify items that willbe impacted by the change.

Helix ALM also includes suspect item flagging, which streamlines and automates change reviews by determining which linked items (requirements, test cases, defects, change requests, etc.) need to be reviewed when a related item changes.

SOFTWARE CONFIGURATION MANAGEMENT

Perforce's configuration management solution, Surround SCM, manages all changes to a product's code base. Surround SCM provides a variety of advanced capabilities for users, including flexible branching and merging, integrated code reviews, line-by-line change history annotation, and more.

Branching and merging provide effective management of product versions through out the product's lifecycle. Surround SCM does not impose a branching process on users — branching configuration depends on a company's needs and business processes.

Integrated code reviews provide a way to request feedback and approval before committing changes to the code base. Reviewers can make comments directly in the code review, while the workflow engine manages the review and approval process.

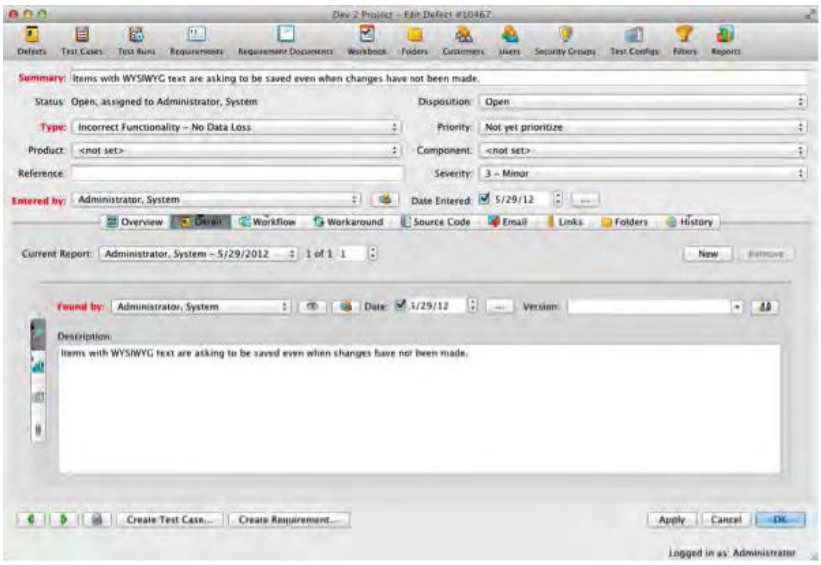

Figure 5: Helix ALM enables users to track everything about an issue.

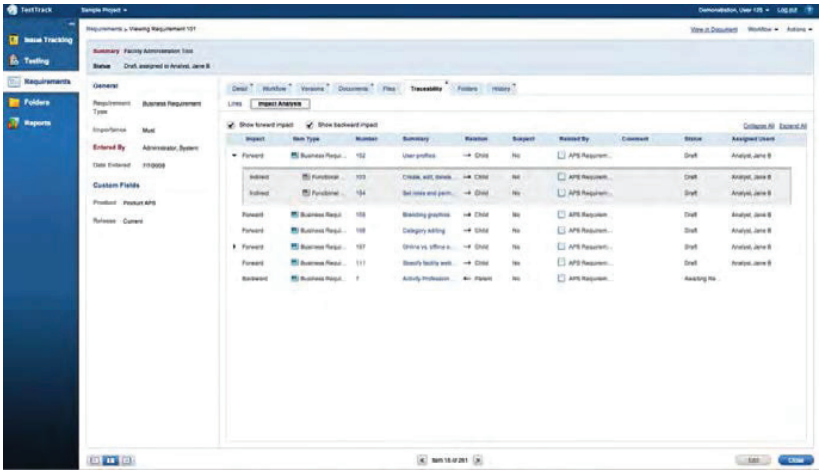

Figure 6: Helix ALM's impact analysis reports make it easy to assess the impact of a requirement change before it is made.

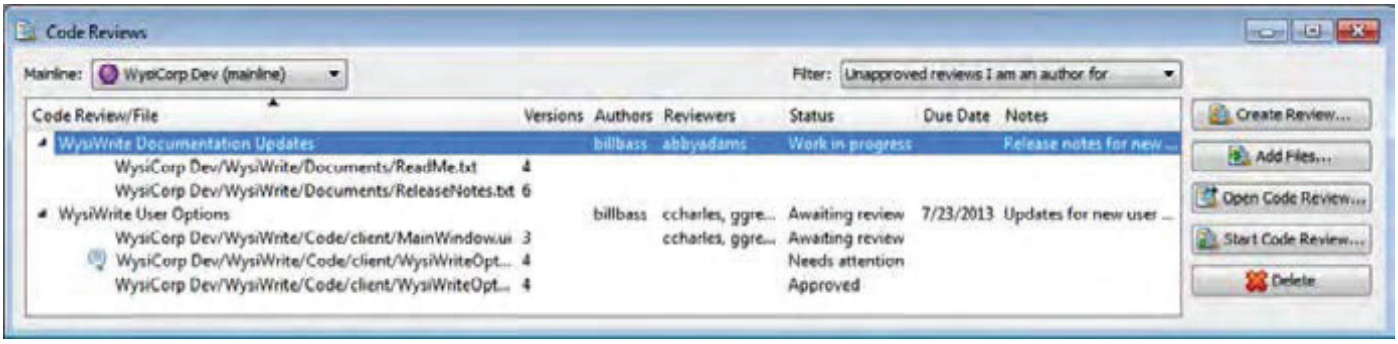

Figure 7: Integrated code reviews provide a way to group related files or changes without affecting current file contents.

Surround SCM's graphical file history window gives users a high-level view of the file history, making it easy to see file changes across different releases and versions. Users can interactively trace a file's history, see what's different between any two versions, and gain insight into source code changes. In addition, they can get a graphical view of the branch structure to see how different product versions relate to each other.

Figure 8: The graphical file history window shows a high-level view of the file history.

TRACEABILITY

The traceability matrix serves in part to "guarantee that all necessary operations have been carried out to demonstrate that the required software systematic capability has been achieved," as required in Part 3 of IEC 61508 (see Table 1).

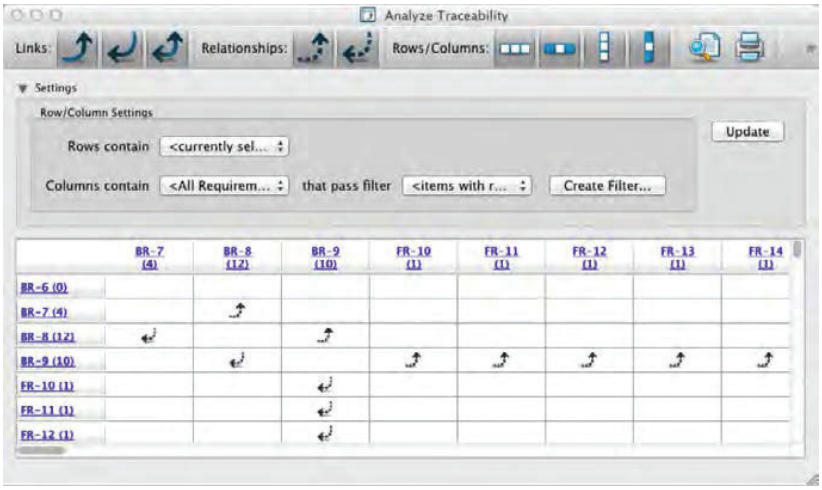

Figure 9: Helix ALM's automated traceability matrix make it easy to quickly perform coverage analysis.

With Helix ALM's traceability features, however, it can be much more than a checked off item on an audit checklist. Helix ALM will generate and maintain a traceability matrix to connect functionality safety requirements with product specifications, help the team estimate how many tests will be needed, provide visibility into the impact of change throughout the product development cycle, and make providing proof of compliance much easier.

Helix ALM's traceability matrix also makes it easy to quickly perform coverage analysis by viewing the relationships between related items. For example, users can check that at least one test case has been generated for each approved requirement in a project.

Automated linking between requirements, risk, tests, and issues makes all of this possible without adding overhead to a team's already busy workload.

REPORTING

Customizable reports and charts help measure impact, burn down rates, track project progress, and measure productivity to stay on top of the project schedule. Helix ALM reports provide realtime insight into every aspect of the project, and enables users to quickly spot trends and identify potential problems before they negatively impact the project.

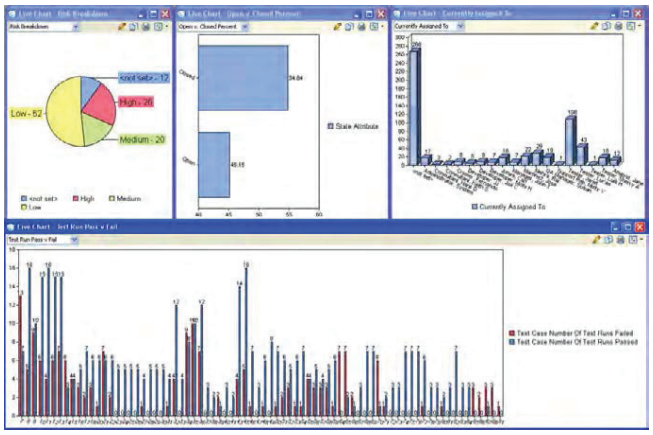

Figure 10: Helix ALM provides real-time reporting across all development and testing artifacts.

WORKFLOW AND PROCESS AUTOMATION

Safety-critical companies have a wide range of artifacts and work items to track — everything from requirements and specifications to test cases and defects, even unique compliance specifications. Using Perforce solutions, organizations can more easily manage all of these assets enterprisewide and at the same time standardize their processes — tying together departments, remote offices, and even customers.

Consistency and predictability are two key focuses for companies today, making sure they deliver products that meet customer needs on time and within budget. On top of that challenge, there's the need to prove regulatory compliance as part of the product delivery process. Centralizing the management of product development assets, and enforcing a consistent process across disparate teams is critical in those kinds of environments.

COLLABORATION

Sharing information is a critical success factor for any product development team, given the nature of today's distributed organizations. Helix ALM's communication and collaboration features ensure team members stay informed of each other's tasks and progress, with all conversations and decisions stored in a centralized repository.

Helix ALM streamlines the development lifecycle with automatic assignments of work items and a powerful rule-based email notification system that keeps team members informed of work assignments, high priority issues to monitor, test failures, and more.

With Surround SCM, end-to-end traceability enables users to release features and fixes rather than individual file changes. By linking code changes to up-stream requirements or issues, Surround SCM enables releases based on all of the changed linked to a specific requirement or defect rather than pushing individual files.

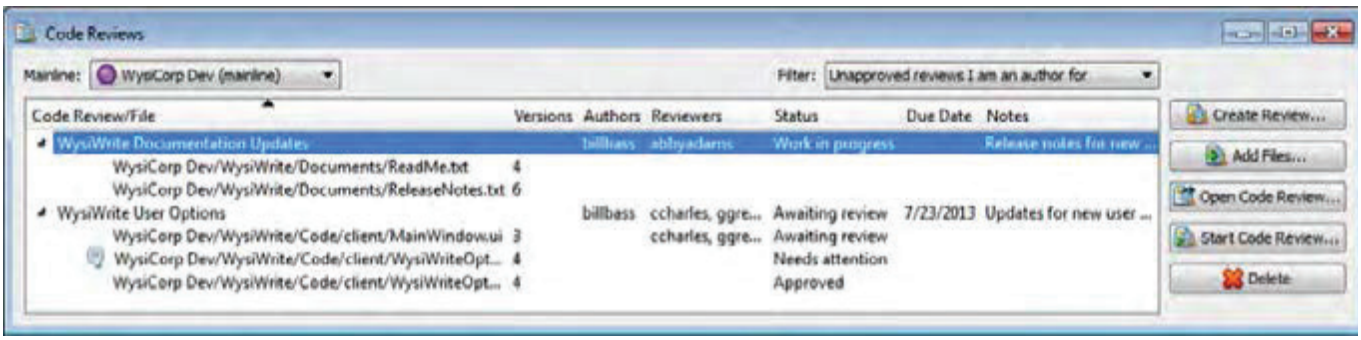

Figure 11: Surround SCM lets users know the true status of files in the change process.

Helix ALM streamlines the development lifecycle with automatic assignments of work items and a powerful rulebased email notification system that keeps team members informed of work assignments, high priority issues to monitor, test failures, and more.

Integrated code reviews provide a way to group related files or changes and request feedback from others without impacting code in production. They know whether a file they are including in the build was code reviewed, can ensure design documents went through the review process, and can control who can make changes to reviewed and approved files.

Conclusion

Functional safety is increasingly challenging. Once deployed into the field, E/E/PE safety-related systems must work dependably. Perforce solutions help developers efficiently design, build, and test these complex systems.

Functional safety touches all parts of our lives, from automobiles to medical products to aerospace products. Unique development challenges surround designing and building these embedded systems, because software is developed independent of the hardware it will eventually run on. Managing this dual track development of complex systems requires good process with strong integration between development teams and across tools improving efficiency and reducing project risk.

With Helix ALM managing all product development and testing artifacts and Surround SCM managing the code and other digital assets, Perforce offers tightly integrated solutions that covers the entire development lifecycle described in IEC 61508-3.

About Perforce

Perforce enables the largest technology teams across the globe to do their best work and innovate at scale. Our solutions solve everyday development challenges around version control, developer collaboration, and project lifecycle management. For more information, please visit www.perforce.com.