expresslogic

Meeting Regulatory Standards for Safety-Critical Embedded Systems

Introduction

We've all seen the frightening stories of Toyota automobiles accelerating out of control or failing to apply brakes properly, leading to injuries and death. Like all modern automobiles, Toyota employs microprocessors and related software to control various systems within the car – from anti-lock braking systems (ABS) to electronic fuel injection, and engine control. These are "safety-critical" systems, which must perform correctly, as intended, in order to assure the safety of the passengers and other vehicles around them.

While Toyota's automobiles have not been shown to have experienced any electronic or software system failure, some speculate that indeed, this is exactly what has led to many of the malfunctions that drivers have experienced. Clearly, whether this is true or not in the case of Toyota, such systems endanger life and limb if they were to actually fail.

For this reason, governments around the world have stepped in to define rigorous standards which safety-critical systems must meet. And, not just for automobiles, where electronic systems have been subject to less regulatory control than other types of systems. In the areas such as medical equipment, avionics, and industrial control, regulations abound and developers must plan to provide evidence of compliance before they can bring new products to market.

Software for Safety-Critical Systems

Software used in safety-critical systems is, of course, a key element in the correctness of the system's operation. Most commonly, this software consists of an application running on top of an operating system. In some cases, the product manufacturer uses an in-house operating system, and in other cases, a commercial RTOS. In all cases, the final system must perform flawlessly, since any malfunction might result in injury or death.

Regulatory Agencies for Key Industries

Because of the criticality of such systems to operate safely, various government-sponsored agencies and independent technical standards organizations have become involved in defining regulations for safety-critical software. These agencies include:

a) **Industrial Systems**: The International Electrotechnical Commission (IEC), a worldwide organization for standardization, promotes international co-operation on all questions concerning standardization in the electrical and electronic fields.
   - IEC 61508, the international standard for electrical, electronic and programmable electronic safety related systems, sets out the requirements for ensuring that systems are designed, implemented, operated and maintained to provide the required safety integrity level (SIL). IEC 61508 has been adopted in the UK as BS EN 61508.

- IEC 61511 Process industries
- IEC 61513 Nuclear power plants
- IEC 62061 Machinery sector
- IEC 61800-5-2 Power drive systems.

b) **Aviation Systems**: RTCA, Inc. is a private, not-for-profit, US corporation that develops consensus-based recommendations regarding communications, navigation, surveillance, and air traffic management (CNS/ATM) system issues. RTCA functions as a Federal Advisory Committee, whose recommendations are used by the US Federal Aviation Administration (FAA) as the basis for policy, program, and regulatory decisions. The RTCA's DO-178B, and its virtually identical European Union counterpart, EUROCAE's ED-12b, defines the standard by which the FAA certifies software for use in aviation-related applications. DO-178B defines 5 levels of criticality:
   - Level A - Catastrophic - Failure may cause a crash
   - Level B - Hazardous - Failure has a large negative impact on safety or performance, or reduces the ability of the crew to operate the aircraft due to physical distress or a higher workload, or causes serious or fatal injuries among the passengers
   - Level C - Major - is significant, but has a lesser impact than a Hazardous failure
   - Level D - Minor- failure is noticeable, but has a lesser impact than a Major failure
   - Level E - No Effect - Failure has no impact on safety, aircraft operation, or crew workload

c) **Medical Systems**: The US Food and Drug Administration's (FDA) Center for Devices and Radiological Health (CDRH) is responsible for new medical devices brought to market in the US, and for recall and examination of existing devices suspected of malfunction. In the UK, the Medicines and Healthcare Products Regulatory Agency (MHRA) regulates medical devices. International Standard IEC 62304 addresses quality management and corresponding general aspects for medical devices.

d) **Transportation/Rai**l: CENELEC governs European railway standards, and these standards are beginning to make their way into the North American railway and public transport market. The CENELEC standards EN 50126, EN 50128 and EN 50129 are generally recognized as acceptable with respect to applicable elements of safety analysis. EN 50126 is often called the "RAMS" standard, since it deals with Reliability, Availability, Maintainability and Safety for the entire railway system. EN 50129 applies to safety-related electronic control and protection systems. EN 50128 applies to safety-related software for railway control and protection systems. The standards EN 50128 and EN 50129 represent the railway application-specific interpretation of the international standard series IEC 61508.

Common Elements

All international safety-critical software standards incorporate common elements that apply to all software systems, regardless of their end application. While the different standards have their own particular phraseology and individual features, they all generally require that software be supported by rigorous documentation of the following elements:

- **Process methodology** outlines how the software system is designed, and is broken down into several sub-categories:
   - ✓ Planning
   - ✓ Design
   - ✓ Development

- ✓ Requirements
- ✓ Verification
- ✓ Configuration management
- ✓ Quality assurance

- **Code** refers to the source code produced by the developer or development tool and it includes all system and application source code, test code, scripts, and object code.

- **Test** includes specific tests performed to verify the correct operation of the code, as well as its ability to achieve all design goals and system requirements. Testing includes code coverage and analysis to insure that all program instructions are tested. Finally, unit/white-box, integration/black-box, and final acceptance testing generally are included.

- **Results** consists of complete results of all tests compiled into a unit and integration test report.

Express Logic's ThreadX® RTOS for Safety-Critical Systems

Express Logic's ThreadX® RTOS has been used in safety-critical products within the fields of avionics, medical devices, transportation, and industrial control equipment. Developers facing IEC, FDA, or other regulatory approval requirements for safety-critical operation now have 3 solutions from Express Logic to make their job easier:

1. TUV Off-the-Shelf Certification
2. UL Off-the-Shelf Certification
3. Certification Pack™ Turnkey Certification Services

Each of these solutions offers benefits for developers of safety-critical systems.

1. TÜV Off-the-shelf Certification

ThreadX has been certified by SGS-TÜV Saar for use in safety-critical systems, up to SIL-4, according to:

- IEC-61508
- IEC-62304
- ISO 26262
- EN 50128

The certification confirms that ThreadX can be used in the development of safety-related software for the highest safety integrity levels of IEC 61508, IEC 62304, ISO 26262 and EN 50128 for the "Functional Safety of electrical, electronic, and programmable electronic safety-related systems." SGS-TÜV Saar,

formed through a joint venture of Germany's SGS-Group and TÜV Saarland, has become the leading accredited, independent company for testing, auditing, verifying and certifying embedded software for safety-related systems worldwide. The industrial safety standard IEC 61508, and all standards that are derived from it, including IEC 62304, ISO 26262 and EN 50128, are used to assure the functional safety of electrical, electronic, and programmable electronic safety-related medical devices, process control systems, industrial machinery, automobiles and railway control systems.

SGS-TÜV Saar has evaluated the relevant parts of Express Logic's modified waterfall development process for ThreadX v5.6, with phase overlap and phase blending, to ensure that best development practices have been followed at these stages:

- Requirements Management
- Design
- Implementation
- Verification
- Maintenance

SGS-TÜV Saar, using an extensive test suite, rigorously tested all services and features of the ThreadX RTOS. The ThreadX test suite, comprised of a large number of application simulations, effectively performs functional "black box" testing over the entire ThreadX RTOS. The tests exercise 100 percent of the generic ThreadX C code, which is validated by using code coverage analysis tools. Express Logic's ThreadX Safety Manual documents these quality assurance measures, which enable developers to use ThreadX in safety-critical software development for even the most rigorous Safety Integrity Level (SIL), according to IEC 61508, IEC 62304, ISO 26262 or EN 50128 without further qualification.

2. UL Off-the-shelf Certification

ThreadX® has been recognized by UL for compliance with UL 60730-1 Annex H, CSA E60730-1 Annex H, IEC 60730-1 Annex H, UL 60335-1 Annex R, IEC 60335-1 Annex R, and UL 1998 safety standards for software in programmable components. UL is a global, independent, safety-science company with more than a century of expertise innovating safety solutions, ranging from the public adoption of electricity to breakthroughs in sustainability, renewable energy, and nanotechnology.

"*ThreadX is the first RTOS to achieve UL recognition to the standards UL 60730-1, CSA E60730-1, IEC 60730-1, UL 60335-1, and IEC 60335-1," commented Jason R. Smith, Staff Engineer of UL. "We are excited that Express Logic now is able to apply the UL mark to its products, giving home appliance manufacturers confidence that they can use ThreadX and be assured of its compliance with these important safety standards*."

Along with IEC/UL 60730-1, which has requirements for “Controls Using Software” in its Annex H, the IEC 60335-1 standard describes the requirements for “Programmable Electronic Circuits” in its Annex R. IEC 60730 Annex H and IEC 60335-1 Annex R address the safety of MCU hardware and software used in appliances such as washing machines, dishwashers, dryers, refrigerators, freezers, and ovens. Building on the UL1998 foundation, additional requirements addressing the issues of software safety in programmable components for home appliances have now been added to the latest editions of the UL 60730/60335 standards. ThreadX is the first to have satisfied those new requirements.

3. Certification Pack™ Turnkey Certification Services

Manufacturers of medical, avionics, and industrial devices have development teams that are fully capable of generating the documentation required to comply with these safety-critical standards, as required by applicable regulations. In fact, many of them have done so for years. However, there are some aspects of this work that developers would like to avoid or that pose challenges.

First of all, safety-critical software typically employs a real-time operating system for control and management of the application on a given processor. Generally, such applications involve multiple application tasks, or threads, and a priority-based real-time scheduling OS, with interrupt capability for real-time responsiveness. A commercial RTOS provides these functions with an easy-to-use application programming interface (API) that can save developers substantial time in product development.
If a commercial RTOS is used, the developer is challenged to comply with the regulatory requirements that call for documentation and testing of software that was developed by an independent entity. In addition, the time required to generate and organize all the RTOS-related documentation might represent a significant portion of the project schedule.

Moreover, some commercial RTOSes are not delivered with full source code, making them even more challenging to document. Still, if the RTOS is delivered with full source code, and if it is manageably small, then it is feasible for the developer to complete the regulatory tasks.

Express Logic’s customers have successfully produced the required documentation as required by governing agencies for the ThreadX RTOS which has been used in many medical, industrial, and avionics systems. This process required additional time and it increased their costs.

For many companies, using a 100% turnkey solution to the demands of regulatory compliance offers a better way to managing regulatory compliance. Express Logic’s Certification Pack™ consists of all the RTOS design, code, test, and results documentation that each standard requires, fully prepared and guaranteed to be accepted by the governing agency. Using such a turnkey solution takes a huge burden off developers and allows them to focus on their own software.

Certification Pack solutions for the RTOS are 100% turnkey, and available for virtually all safety-critical software standards in the areas of medical, avionics, industrial, and transportation. Developers who wish to tackle part of the effort in-house are able to do so as well. Developers should make the trade-off between efficient use of in-house personnel for this effort over the cost savings of using a commercial package prepared for the RTOS.