Introduction to Functional Safety

BlackBerry QNX Professional Services

With the increase in automation and consolidation in automotive, medical, rail and industrial embedded systems comes the need to ensure these systems can provide automatic protection against failures. Over the last few years, several functional safety standards have been introduced to ensure software development practices align with safety systems.

For the last 10 years, BlackBerry® QNX® has been delivering software products certified to the highest safety integrity levels according to ISO 26262 and IEC 61508. We've also provided engineering services, working closely with our clients to understand their safety goals, and have brought custom developed components to certification with TUV® Rheinland.

To help you explore the complex landscape of functional safety and safety certification, we have developed the Introduction to Functional Safety course. The course material was developed by Chris Hobbs, functional safety expert and principle developer at BlackBerry QNX, based on his book "Embedded Software Development for Safety-Critical Systems." This course is intended for development managers or engineers who have to develop software to meet the requirements of a safety standard.

Introduction to Functional Safety (Five-Part Course)

This introductory training course covers the basics of functional safety as it applies to embedded system design. This course is a subset of the full twelve-part functional safety course and covers:

Part 1: Introduction to functional safety concepts and standards
This session provides an overview of concepts and industry-specific safety standards such as IEC 61508, IEC 62304, EN 5012X, ISO 26262. It also discusses the changing balance between functional safety and Safety of the Intended Functionality (SOTIF).

Part 2: The Safety Case
This session covers the creation of a safety case and demonstrations of the various notations used to present an argument including Goal Structuring Notation, Bayesian Belief Networks, and the SACM metamodel.

Part 3: Safety Culture
This session covers the concept of a safety culture including hazard and risk analysis (HARA) and the derivation of the safety requirements and residual risks from it. It also covers failure analysis within the context of SOTIF.

Part 4: Formal and Semi-Formal Methods
This session covers the use of formal methodologies to reduce testing burden. The usefulness of this approach, as well as a review of tools that perform formal verification on a model, will be discussed.

Part 5: Design Patterns
This session covers common design patterns used in safety critical systems such as anomaly detection, replication and diversification. Common patterns such as the safety bag will be covered, as well as an overview of less common techniques (recovery blocks, coded processing).

Service Package Details

Led by a BlackBerry QNX functional safety expert and delivered in live virtual sessions, this course includes:

- Five 90-minute live sessions held over 2.5 consecutive days
- Course workbook with exercises and pointers to the textbook for more details on the topic
- We recommend a maximum of 20 people to enable effective sessions

This course can be customized to focus on the standards or industry of interest to the client including:

- Industrial (IEC 61508)
- Medical (IEC 62304 and ISO 14971)
- Railway (EN 5012x, EN 50657)
- Road Vehicles (ISO 26262, UL 4600, ISO/PAS 21448)

About BlackBerry® QNX®

BlackBerry QNX is a leading supplier of safe, secure, and trusted operating systems, middleware, development tools, and engineering services for mission-critical embedded systems. BlackBerry QNX helps customers develop and deliver complex and connected next generation systems on time. Their technology is trusted in over 150 million vehicles and more than 300 million embedded systems in medical, industrial automation, energy, and defense and aerospace markets. Founded in 1980, BlackBerry QNX is headquartered in Ottawa, Canada and was acquired by BlackBerry in 2010.