

Ensuring the integrity and functional safety of your medical device

Shawn A. Prestridge, Senior FAE

Agenda

- Motivation
- Why should I use a functional safety-certified tool?
- What does it mean if my tool is functional safety-certified?
- Speeding the path to your device's integrity and functional safety certification

Motivation

Challenges with certification



- Need to show repeatable and functional safety-compliant process
- Need to show clear risk management
- Rigorous software verification and validation (V&V) activities
- The IEC 62304 – is the standard which specifies life cycle requirements for the development of medical software and software within medical devices.

Why should I use a
functional safety-certified
tool?

Ensuring integrity and safety



- Certifications make you consider carefully your device's design
 - Defines failure modes and how to recover
 - Makes you think about other failure modes for new device types
- You must outline carefully these modes for review by a certification-granting entity to show you understand the risks and have them mitigated

Solutions for safety-critical applications

Certified toolchain

- A special functional safety edition of IAR Embedded Workbench

Simplified validation

- Functional Safety certificate from TÜV SÜD
- Safety report from TÜV SÜD
- Safety guide

Guaranteed support through the product life cycle

- Prioritized support
- Validated service packs
- Regular reports of known problems



Available for: Validated* according to:

Renesas RX

Renesas RL78

Arm*

IEC 62304

IEC 61508

ISO 26262

EN 50128



FS-certified tools

- When a tool is certified, you are guaranteed that it is well-tested to adhere to industry safety standards
- Allows you to focus on your application development rather than finding/fixing tool-related issues
- It takes removes the tools from your V&V and risk management efforts

Benefits to using tools that are certified



- Reduce liability risks associated with your application
- Reduce odds of product recall
- Reduce number of firmware updates
- Ensure compliance with international standards and requirements

- Protects your company's reputation
- Also protects your company's bottom line

What does it mean if my tool
is functional safety-certified?

Tool certification is important



- It means that your development tool has gone through a rigorous qualification process to ensure that it produces reliable and repeatable results when compiling your code.
- Additionally, it means:
 - Development processes are in place to manage how the tool works with specific requirements put forth by different functional safety standards
 - There are test and quality measures of the tool show validation of compliance with different language standards

Certification also means...



- There are specific processes and metrics in place to handle issues reported from the field and how users are updated about known issues
- A safety manual is provided to show proof-of-compliance with standards and how to operate the development tool to comply with FS standards
- Assessment takes into consideration how many developers are using the toolchain to ensure it has a broad user-base

Speeding the path to your
safety certification

How does a FS-certified tool help?



- The simple answer is that it removes the requirement that you have to prove your toolchain complies with the safety standard.
- It also means that your test-and-fix phase of the Software Development Lifecycle (SDLC) can focus on finding bugs in your source code instead of wondering if a compiler issue is causing your problems.
- Certified service packs mean that you don't have to recertify the tool to get added functionality to your toolchain.

What do I get with a FS-certified version?



- A complete build chain that is certified by TÜV SÜD to comply with the requirements for tools selection in IEC 62304 (IEC 61508 – Arm*)
- A report that accompanies the certificate that states under what circumstances the certificate is valid
- A test report that shows how the tool was tested to demonstrate compliance

What do I get with a FS-certified version?



- A compiler that supports C89, C11, and C++14 languages (Note that the safety standards do not recommend using exceptions and RTTI in C++)
- Prequalified service packs for your FS tool to maintain certification and support for the life of the FS version (as long as there are paying customers under support contract for that version)
- Regular updates on known issues

Ensuring safety and integrity



- Certifications are easier to achieve when you can prove that your code conforms to a coding standard (such as MISRA).
- Testing reports show that the overall number of defects in the software is low, despite many hours of testing and proves maturity of your development organization.
- Code analysis also shows that your results are repeatable because you have a process in place to find and fix defects.

Code analysis



Be sure to attend our seminar on code analysis!

10:30 on Feb. 27

15:00 on Feb. 28

13:00 on Mar. 1



Summary



- FS-certified tools are exceedingly well-tested
- FS-certified tools help you to focus on just your application
- FS-certified tools help speed the path to your certification
- Code analysis tools help prove your design's safety and integrity

Want to learn more?



- Get scanned to have this presentation emailed to you.
- Visit IAR Demo Space to get a demo of our technology.

Thank you for your attention!