



### **Industrial Safety Fact Sheet**

**Green Hills Software provides a complete platform for Industrial Devices with safety requirements, including a safety certified Real-Time Operating System and best-in-class development tools for the IEC 61508 safety critical market.**

Green Hills Software, Inc. is the technology leader for Real-Time Operating Systems (RTOS) and Device Software Optimization (DSO) for 32- and 64-bit embedded systems. Our technology and products enable electronic equipment developers to produce embedded software that is ***totally reliable***, yields ***maximum performance***, is ***absolutely secure*** and can be developed ***in the least time*** and with the ***lowest*** investment in ***development and manufacturing cost***.

A 23-year veteran in the embedded software industry, Green Hills Software has a proven history of satisfied customers in the process control industry, including Honeywell Controls, Emerson Process Management, Ingersoll-Rand, Serveron and Pilz. Representative customer applications include remote surveillance equipment, on-line transformer monitor, alarm and sensor devices, railway signaling equipment, emergency stop relay, and programmable safety systems.

#### **The Market**

The industrial control market has strict requirements for device safety and security due to the often catastrophic nature of failures in these systems. The software that controls devices used in these industries must have the utmost reliability and go through stringent analysis and testing before being deployed. Developing and deploying software for these devices has traditionally been a time-consuming and expensive process.

The Green Hills Platform for Industrial Safety provides an advanced solution for building safe and reliable systems that require certification up to the demanding IEC 61508 Safety Integrity Level 3 (SIL3). This complete solution consists of a safety certified real time operating system, supporting evidence for safety certification, and integrated middleware, tools and services that address the growing challenges around rising product cost, risk, and time-to-market to develop and deploy these products.

#### **IEC 61508**

IEC 61508 is an international standard for the functional safety of programmable electronic systems. Well established in the industrial process control and automation industry, IEC 61508 is gaining a foothold in automotive, heavy machinery, mining and other applications where safety and reliability are paramount. Meeting IEC 61508 requirements involves a systematic development process, emphasizing requirements traceability, criticality analysis and validation. The SIL3 rating is considered the highest level of risk reduction achievable using a single processor.

The SIL levels are based on the probability of a dangerous failure over time. It is important to note that IEC 61508 allows for independent assessment of subsystems and components. The following subsystems and components can be classified into the these categories:

- Safety Critical: single fault can result in a dangerous failure
- Safety Relevant: a single fault in combination with a second fault can result in a dangerous failure
- Interference Free: faults can not cause a dangerous failure

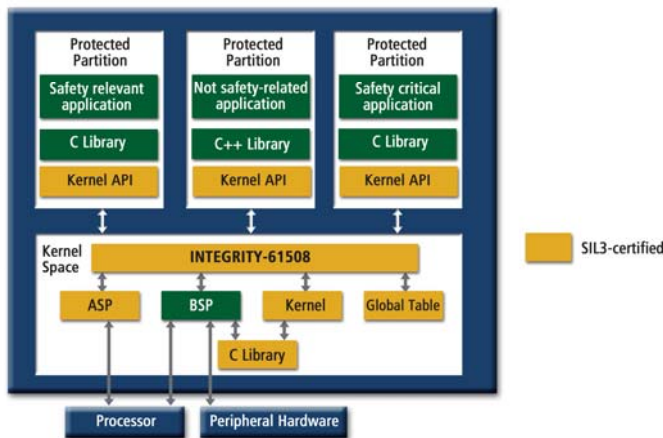
Safety Critical components require the most scrutiny and tend to be the most expensive in terms of time, cost and certification effort.

### Green Hills Platform for Industrial Safety

Certifiable safety and reliability and the lowest possible cost for certification and development are key requirements for products in this segment, which control robots, electrical transmission lines, hazardous gas monitoring, and emergency shut down.

#### INTEGRITY-61508

Green Hills Software’s royalty-free INTEGRITY-61508 is the first RTOS that provides complete support for multiple levels of IEC 61508 functional safety running concurrently on a single microprocessor. The INTEGRITY-61508 architecture allows multiple software applications to share a common hardware platform and is designed that any error in one application cannot prevent another application from continuing to operate.



As such, the INTEGRITY-61508 product can be configured for complete time, space, and resource partitioning between applications operating on the same hardware platform. In the safety critical arena, this means that you can have multiple applications on a single target processor operating at different levels of functional safety. With this architecture, it is possible to divide your

system into components at various criticality levels and be assured that a failure in an Interference Free component cannot cause a failure in a Safety Critical component. Furthermore, INTEGRITY-61508 does not lock you into a single processor family for certification. INTEGRITY-61508 is certified to run on all of the most common processor architectures available today.

INTEGRITY-61508 also provides the end user with a Safety Manual that outlines an extremely robust set of Application Programming Interfaces (APIs) that are available to developers for use of applications demanding the highest level of safety criticality (SIL3). Additionally included are the certificate for TÜV SIL3 certification for INTEGRITY-61508, the TÜV certification report and defect notification services.

#### *61508 related documentation and services*

Optional 61508 related documentation and services include INTEGRITY-61508 kernel lifecycle data, INTEGRITY-61508 source code, custom development and assistance in customers' end product certification efforts, Board Support Package (BSP), device driver development and certification assistance, and on-site audit support.

#### *Optional Middleware*

INTEGRITY-61508 supports the following extensive set of optional middleware: file systems, USB, networking protocols, security protocols and more. This middleware can run in non-safety related partitions of the certified system.

#### *Advanced Development Environment*

Green Hills Software's MULTI Integrated Development Environment and hardware-assisted debugging probes provide a complete environment to develop, debug, and optimize industrial device software. The SuperTrace Probe and TimeMachine Debugger have revolutionized debugging by allowing software developers to analyze trace data captured in real-time using a familiar application debugger, without interfering with the processor's execution.

Green Hills Software also offers supporting documentation for its rich development environment in the form of a confidence in use assessment report. This assessment report describes how MULTI meets the IEC 61508 requirements for development tools and programming languages.

#### *Certified Safety at a Lower Cost*

The Green Hills Platform for Industrial Safety enables the consolidation of traditionally distributed systems and software onto a single microprocessor. In the past, manufacturers had to certify all software running on a processor to the most stringent safety level required by any component. Consequently, "federated" distributed systems had to be deployed to physically separate software at different functional safety levels. While this approach minimized certification cost and risk, it increased the overall system cost and complexity. In contrast, with the innovative secure partitioning capability of the INTEGRITY-61508 RTOS, software—from non safety-related through safety critical—can be partitioned on a single processor. Each partition can then be certified at its appropriate Safety Integrity Level, eliminating the need for separate physical systems or to certify code to a safety level beyond what is required.

The baseline for INTEGRITY-61508, the INTEGRITY RTOS, has unmatched reliability and security credentials. It is the only commercially available, partitioned operating system that has been used in applications certified by the Federal Aviation Administration (FAA) to the highest level required for flight-critical avionics systems. The INTEGRITY RTOS has also been designed into systems for the U.S. government that require the highest level of security certification.

#### **Staying on Top of Industry Needs**

Green Hills Software has established a deep line of products and services that address a number of industries with the most stringent safety and security requirements. By providing the Platform for Industrial Safety, Green Hills expands on its mature offerings for the benefit of customers in the demanding industrial control and process automation industry.

**Contact**

Barbel French

Tel. 805.965.6044 ext. 220

Email: [bfrench@ghs.com](mailto:bfrench@ghs.com)

[www.ghs.com](http://www.ghs.com)

Green Hills Software, the Green Hills logo, MULTI, INTEGRITY, *veIOSity*, SuperTrace, and TimeMachine, are trademarks or registered trademarks of Green Hills Software, Inc. in the U.S. and/or internationally. All other trademarks are the property of their respective owners.