BUILDING FUNCTIONAL SAFETY PRODUCTS WITH WIND RIVER VXWORKS RTOS

Alex Wilson
Director, Market Development
For over 30 years, Wind River has helped the world’s technology leaders power generation after generation of the safest, most secure devices in the world.
DIGITAL BUSINESS TRANSFORMATION

Business Drivers

- New approach for business strategy
- Increased efficiency, safety, resource sustainability
- Need for smart maintenance approaches

The Use of Technology to Radically Improve the Performance or Reach of Enterprises
DIGITAL TRANSFORMATION

Business Impact

- Data-enabled intelligent systems
- Lifecycle costs
- Safety while enabling connectivity
- Security maintenance

Industrial IoT
The future is software defined …
Functional safety
Cybersecurity
Equipment Under Control (EUC): Industrial plant, e.g., welding robotics
Programmable Electronics (PE): Hardware + software
Safety Function: A function that is carried out by a (safety-related) system to minimize risks with the goal of achieving and/or maintaining a secure state for the EUC when a pre-defined dangerous incident is taken into account.
FUNCTIONAL SAFETY APPLIES ACROSS MULTIPLE SEGMENTS

- Process Automation: Safety Controllers, Safety PLC
- Control Automation: Robot Controllers, Manufacturing Systems
- Transportation: Signalling Systems, Control Systems
- Energy: Production Systems, Distribution Systems
SAFETY

The system must not harm the world

Matures and gets more stable over time

SECURITY

The world must not harm the system

Becomes more challenging over time
VxWORKS
Real Time Operating System
VxWORKS CORE PLATFORM

Development Tools
- Compiler & Toolchain
- Full Source Code
- Workbench 4 IDE
- Linux & Windows

Middleware and Application Support
- Network Stack
- USB Stack
- Filesystem
- Inter-Process Communication

Operating System
- 32 and 64 Bit
- Uniprocessor and SMP

Architecture and BSP
- Intel, ARM, PPC
- Atom, QoriQ, ...
- Drivers for Ethernet, USB, ...
VxWORKS FOR SAFETY-CRITICAL SYSTEMS

- General Purpose OS
- Extensive Middleware
- Intel, ARM and PPC

- Time & Space Partitioning Module
- Additional Toolchain for Cert Kernel build
- Certifiable API Subset
- All VxWorks architectures

- Cert Evidence up to DO178C Level A and IEC61508 SIL 3
- Verification Test Harness
- Verified OS Binaries
- Architecture-specific

VxWorks Core Platform
Safety Profile
Certification Evidence
VxWORKS CORE VERSUS SAFETY PROFILE

VxWorks

- USB Stack
- OpenGL Stack
- File System

Safety Profile

- Cert File system *
- Cert Network Stack *

OS Libraries

Cert Subset Libraries

Architecture Adapter

Cert Kernel Architectures

BSPs, Drivers

* Cert Filesystem/Network Stack not yet available on VxWorks 7
## CERTIFICATION STANDARDS

<table>
<thead>
<tr>
<th>Market</th>
<th>Standards</th>
<th>Area</th>
</tr>
</thead>
<tbody>
<tr>
<td>Industrial</td>
<td>IEC 61508</td>
<td>Functional Safety</td>
</tr>
<tr>
<td>Automotive</td>
<td>ISO 26262</td>
<td>Functional Safety</td>
</tr>
<tr>
<td>Nuclear</td>
<td>IEC 60880</td>
<td>Safety</td>
</tr>
<tr>
<td>Rail</td>
<td>EN 50128</td>
<td>Safety</td>
</tr>
<tr>
<td>Medical</td>
<td>IEC 62304</td>
<td>Safety, Software Lifecycle</td>
</tr>
<tr>
<td>Aviation</td>
<td>DO-178C</td>
<td>Safety</td>
</tr>
<tr>
<td>All Markets</td>
<td>IEC 27034</td>
<td>Security, Secure Dev. Lifecycle</td>
</tr>
<tr>
<td>All Markets</td>
<td>IEC 15408</td>
<td>Security, Common Criteria</td>
</tr>
<tr>
<td>Industrial</td>
<td>IEC 62443</td>
<td>Security for Industrial Devices</td>
</tr>
</tbody>
</table>
RULES OF THUMB FOR QUALITATIVE REQUIREMENTS

Zones of Similar Qualitative Requirements

Zone A

Zone B

- DAL A
- DAL B
- DAL C

- SIL4
- SIL3
- SIL2
- SIL1

ARP4761
EN 5012x
IEC 61508
USING VXWORKS FOR FUNCTIONAL SAFETY
SIMPLE SAFETY SYSTEM

VxWorks Safety Profile used Natively

- Simple Safe / non-Safe use case
- Segregated non-Safe application
- All resources under the control of VxWorks Safety profile.
VIRTUALIZATION CONFIGURATION

- Single safety application per core
- Separated non-Safe application
- Device redirect by Hypervisor/Hardware
- Performance impacts easily measured against single core
FUTURE CONFIGURATION FOR VIRTUALIZATION

- Multiple cores per application
- Separated safety applications
- Separated non-Safe application
USING COTS TECHNOLOGY FOR CERTIFICATION
WHERE DO WIND RIVER & INTEL FIT INTO THE STORY?

Programmable Electronics

- Safety Critical Applications
- Safety Evidence for VxWorks
- Safety Evidence for Drivers & Middleware
- Target Hardware

Customer
- IEC 61508 SIL 3

Wind River COTS
- IEC 61508 SIL 3

Wind River Professional Services

Intel Functional Safety CPU
WIND RIVER ENGAGEMENT IN THE OVERALL FRAMEWORK

**Part 1**
- Development of the overall safety requirements (concept, scope definition, hazard and risk analysis)
  - 7.1 to 7.5

**Part 1**
- Allocation of the safety requirements to the E/E/PE safety-related systems
  - 7.6

**Part 1**
- Realization phase for E/E/PE safety-related systems

**Part 3**
- Realization phase for safety-related software

**Part 2**
- Installation and commissioning and safety validation of E/E/PE safety-related systems
  - 7.13 and 7.14

**Part 1**
- Operation and maintenance, modification and retrofit, decommissioning or disposal of E/E/PE safety-related systems
  - 7.15 to 7.17

**Part 5**
- Risk based approaches to the development of the safety integrity requirements

**Part 7**
- Overview of techniques and measures

**Part 6**
- Guidelines for the application of parts 2 and 3

**Technical Requirements**

**Other Requirements**

- Definitions and Abbreviations
  - Part 4

- Documentation Clause 5 and Annex A
  - Part 1

- Management of Functional Safety Clause 6
  - Part 1

- Functional Safety Assessment Clause 8
  - Part 1

© 2017 WIND RIVER. ALL RIGHTS RESERVED.
# VxWORKS SAFETY MANUAL

Guidance for VxWorks usage in a certified environment

## Standards
- IEC 61508
- Cert authority
  - TÜV
  - Determines compliance with standards

## Best Practices
- Installation instructions
- Build environment
- User interface
- BSP
- Processor
- Error handling

## Guidelines
- APIs
  - RTPs
  - DKMs
  - VIP
  - VSBs
- Restrictions
  - TPs, DKMs, VIP, VSB

## Hazard Mitigation
- Failure mode and effect analysis (FMEA)
- Partitioning Safe inter-process communications
- Hardware hazards
SUMMARY

- Wind River is the industry leader, with over 45% market share and deep corporate support with our parent company, Intel.
- Safety systems minimize risks for failures
- Connected safety systems provide value
- VxWorks provides proven basis for Functional Safety