AN INTEL COMPANY

Use of COTS Operating Systems with Lockstep for Rail Safety

Alex Wilson

Director, Market Development

Wind River UK Ltd

WHEN IT MATTERS,
IT RUNS ON WIND RIVER.

Agenda

- Wind River and Artesyn
- ControlSafe Platform
- VxWorks 653 Operating System
- Future Systems

For more than 30 years, Wind River has helped the world's most recognizable brands power generation after generation of embedded devices.

HERITAGE

- 1981: Founded
- 1993: IPO
- 2009: An Intel Company

LEADERSHIP

- 45% Commercial Market Share
- Broadest Portfolio

SCALE

- 1,900 Employees
- 42,000 Developers

INVESTMENT

- 30+% of Annual Spend Is on R&D
- Rich History of M&A

ARTESYN

*The Former **Embedded Computing & Power** Business of*
Emerson Network Power. Our Heritage Includes Motorola Computer Group, Force Computers, and Astec.

Founded in **1971**

Headquartered in **Tempe, AZ**

$1.1B Revenue in 2016

~20,000 Employees

The **Largest** Installed Base of Open Standard Compute Blades and Systems in the World

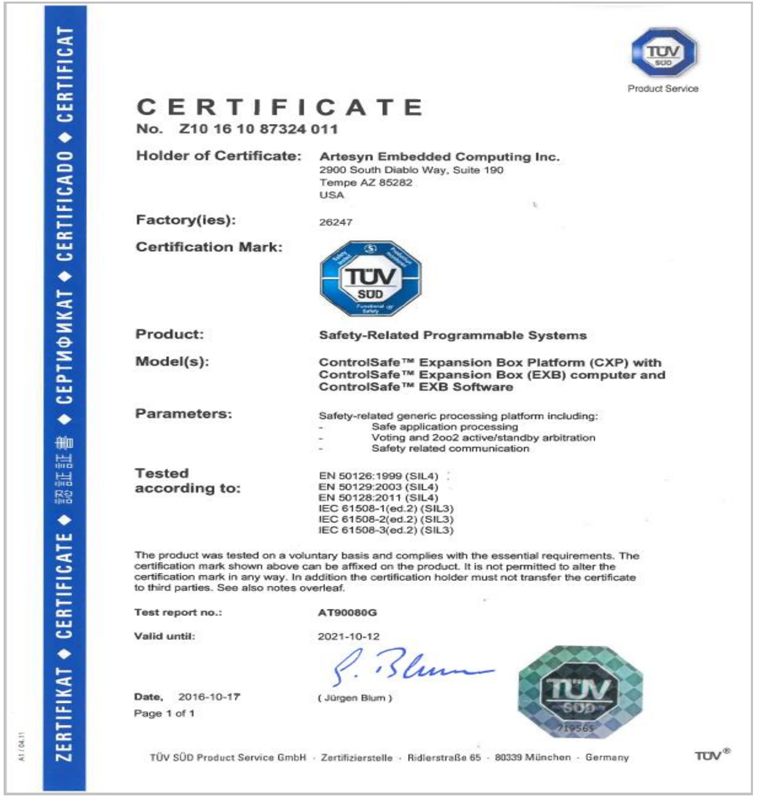
#1 World Leader in OEM Embedded Power

The Global Leader in Power Conversion and Embedded Computing Technologies

Servicing the World's Leaders in Network and Industrial Solutions with COTS Platforms

Now SIL 4-Certified by TÜV SÜD

Cost-Effective COTS Solution Targeting Wayside Applications



ZERTIFIKAT ◆ CERTIFICATE ◆ 認証書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

Product Service

CERTIFICATE

No. Z10 16 10 87324 011

Holder of Certificate: **Artesyn Embedded Computing Inc.**
2900 South Diablo Way, Suite 190
Tempe AZ 85282
USA

Factory(ies): 26247

Certification Mark:

Product: **Safety-Related Programmable Systems**

Model(s): **ControlSafe™ Expansion Box Platform (CXP) with ControlSafe™ Expansion Box (EXB) computer and ControlSafe™ EXB Software**

Parameters: Safety-related generic processing platform including:
- Safe application processing
- Voting and 2oo2 active/standby arbitration
- Safety related communication

Tested according to:
EN 50126:1999 (SIL4)
EN 50129:2003 (SIL4)
EN 50128:2011 (SIL4)
IEC 61508-1(ed.2) (SIL3)
IEC 61508-2(ed.2) (SIL3)
IEC 61508-3(ed.2) (SIL3)

The product was tested on a voluntary basis and complies with the essential requirements. The certification mark shown above can be affixed on the product. It is not permitted to alter the certification mark in any way. In addition the certification holder must not transfer the certificate to third parties. See also notes overleaf.

Test report no.: **AT90080G**

Valid until: 2021-10-12

J. Blum

Date, 2016-10-17 (Jürgen Blum)

Page 1 of 1

TÜV SÜD 719565

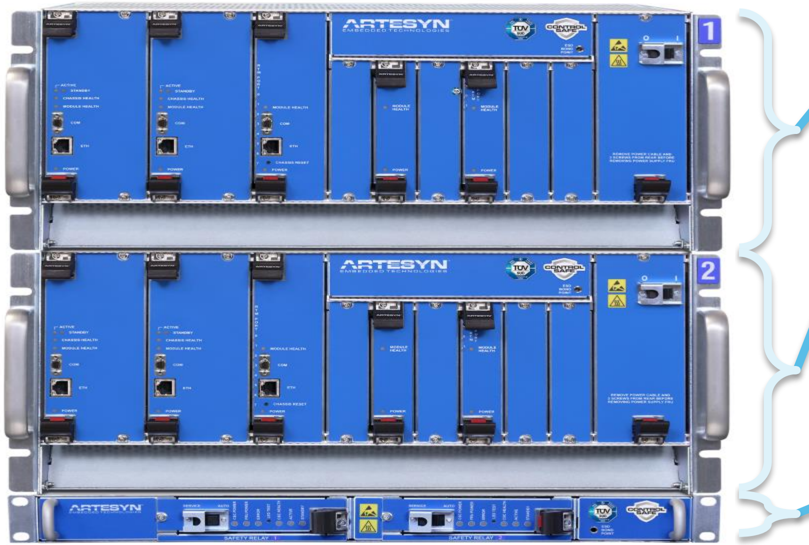
A1 / 04.11

TÜV SÜD Product Service GmbH · Zertifizierstelle · Ridlerstraße 65 · 80339 München · Germany TÜV®

ControlSafe™ Expansion Box Platform

SIL 4-Certified COTS Fail-Safe and Fault-Tolerant System for Train Control and Rail ßSignaling Applications

ControlSafe Platform (CSP)



ControlSafe Computer (CSC)

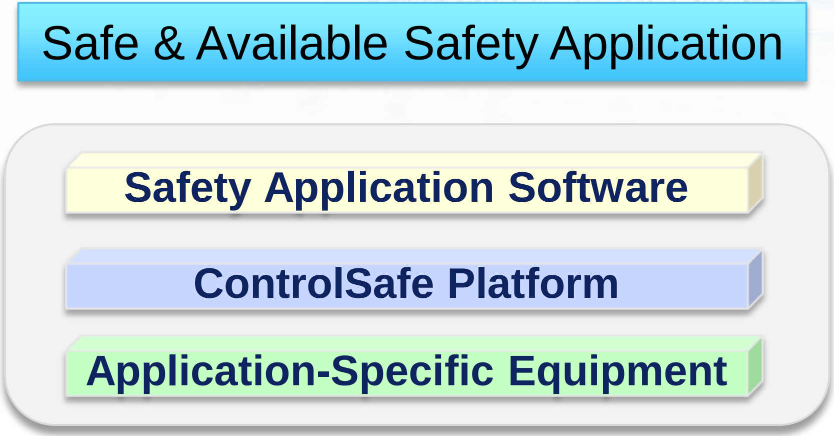
- At the core is the ControlSafe Computer (CSC) with its 2 CPU cards running in data lockstep and voting on all incoming and outgoing transactions.
- Two CSCs form a fault-tolerant system.

Safety Relay Box (SRB)

- The SRB monitors the health of the two CSCs and controls failover operations between them to deliver a fault-tolerant system.

A “Common” Platform Enables Multiple Applications

- Safety application implemented by integrating application software and other application-specific equipment with the CSP
- Sample safety applications:
  - Computer-based interlocking (CBI)
  - Temporary speed restriction server (TSRS)
  - Communications-based train control (CBTC)
  - Train control center (TCC)
  - Radio block center (RBC)
  - PTC (positive train control)


Safe & Available Safety Application

Safety Application Software

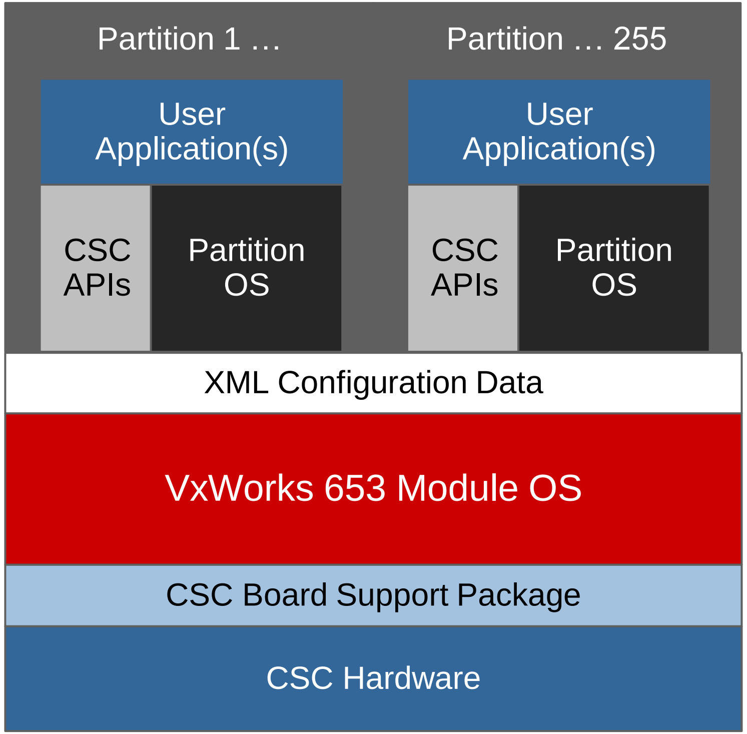
ControlSafe Platform

Application-Specific Equipment

ControlSafe Platform

VxWorks 653 Operating System

- Virtualized operating system
  - Using time and space partitioning
- Two-level scheduler
  - Module OS
  - Partition OS
- Static role-based configuration
- Fault isolation and containment
- Certified to EN 50128



Partition 1 …

Partition … 255

User Application(s)

CSC APIs

Partition OS

User Application(s)

CSC APIs

Partition OS

XML Configuration Data

VxWorks 653 Module OS

CSC Board Support Package

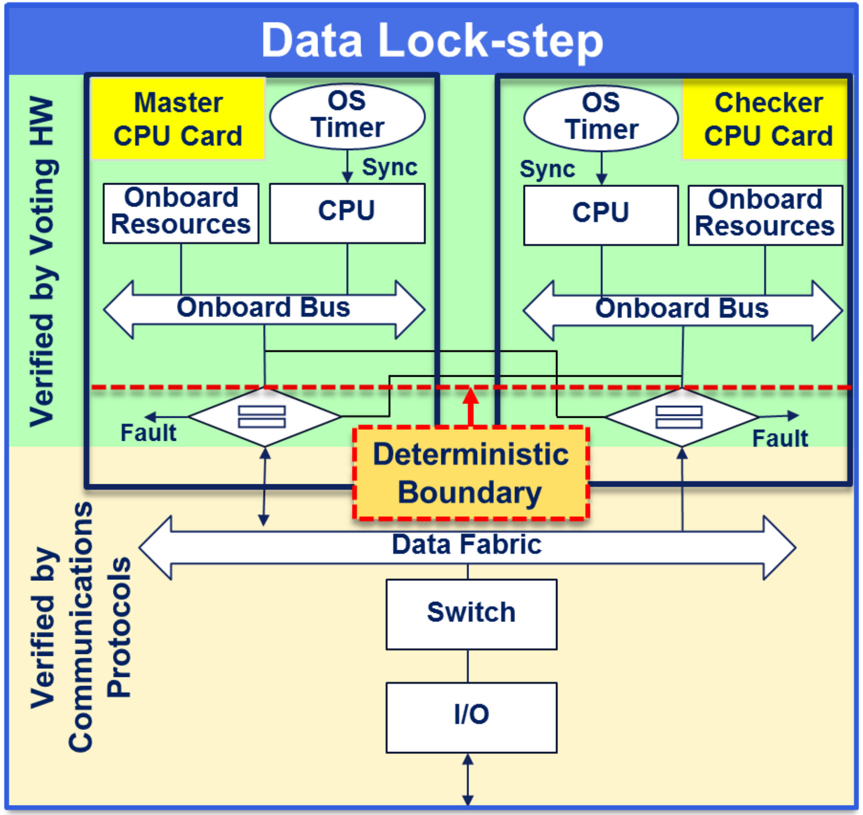
CSC Hardware

Wikimedia.org

VxWorks 653 Safety Pedigree

- 400 Programs
- 200 Customers
- 80 Aircraft

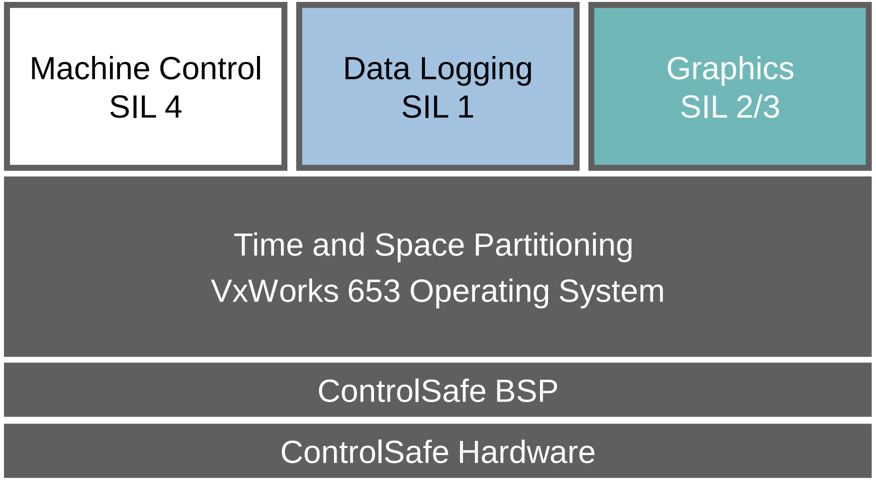
Data Lockstep



- OS services are synchronized between the CPUs
- Voting is done by HW and occurs on every fabric-bound transaction
- Major benefits:
  - Can employ high-performance modern processors
  - Is transparent to application software

Integrated Modular Avionics

- Reduces space, weight, and power
- Enables consolidation and certification of multiple applications
- ARINC 653: Industry specification for integrated modular avionics (IMA)
- Includes API specification of 56 routines
  - Time and space partitioning
  - Inter- and intra-partition communications
  - Health monitoring (error detection and reporting)



Machine Control
SIL 4

Data Logging
SIL 1

Graphics
SIL 2/3

Time and Space Partitioning
VxWorks 653 Operating System

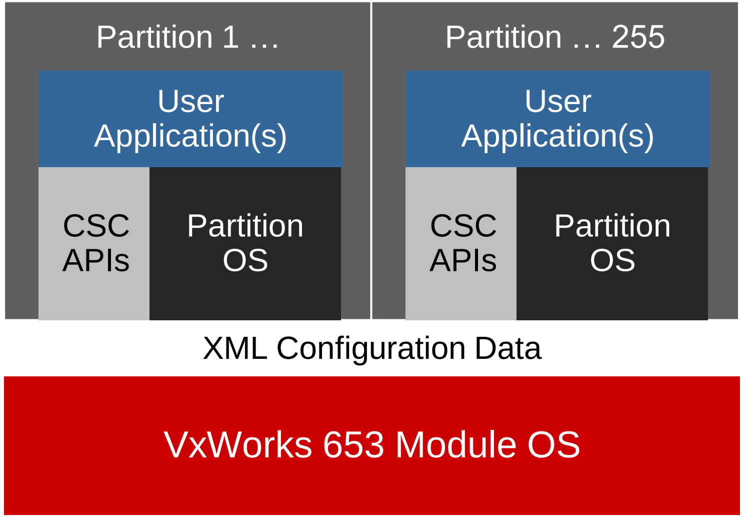
ControlSafe BSP

ControlSafe Hardware

VxWorks 653 Partition Advantages

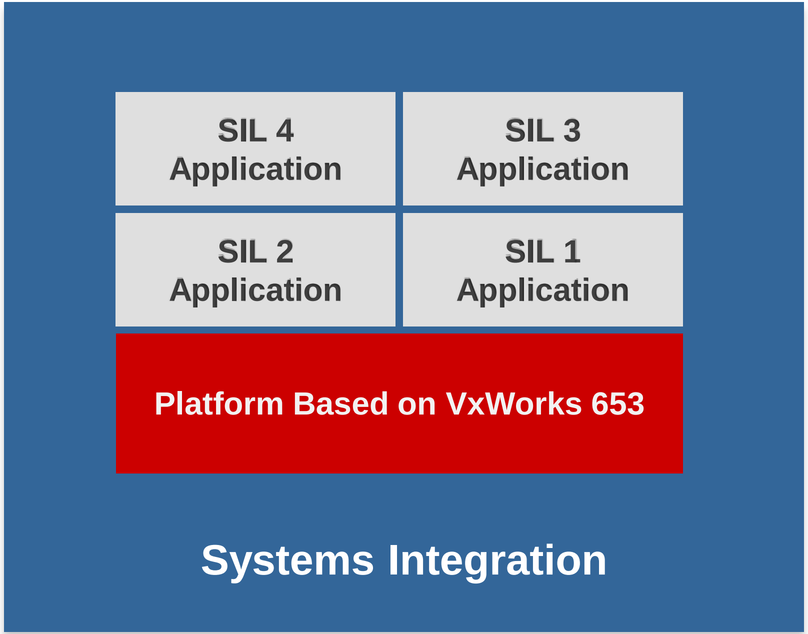
1. Applications protected
   - Execute independently
   - Have their own memory and resources
   - Cannot cause other applications to crash due to an error
2. Buffered inter-partition communication
3. Supports applications of multiple criticalities
   - Safety and non-safety applications
   - SIL 1+2 and SIL 3+4 applications
4. Reduced cost of safety certification
   - Test, certify, and recertify applications independently and asynchronously

Partitions Ensure Applications Are Protected from Each Other



Reduced Cost of Safety Certification

Lifecycle Management



SIL 4 Application

SIL 3 Application

SIL 2 Application

SIL 1 Application

Platform Based on VxWorks 653

Systems Integration

- Independent build, link, and load
- Independent platform, application, and system certification
- Enables
  - Ease of application update
  - Management of platform lifecycle
  - Independent supplier capability
- Lowers
  - Integration cost and effort
  - Application testing cost

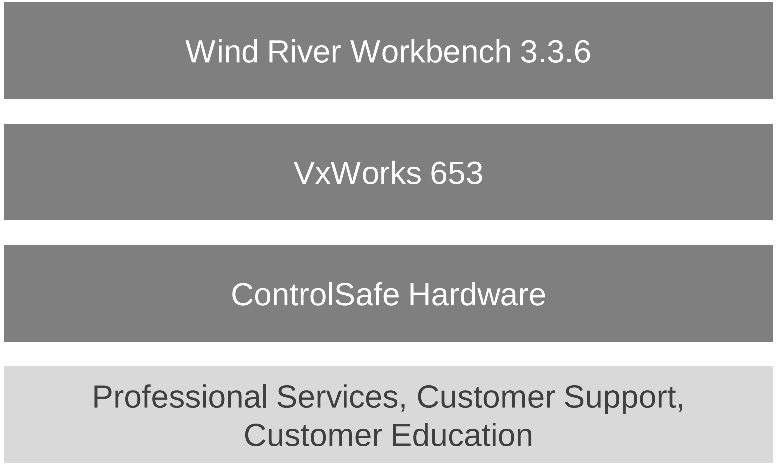
Hierarchical Health Management

- HM framework supports
  - Process level
  - Partition level
  - Module level
- HM framework allows developers quick start
  - Debug handlers provided to facilitate initial bring-up and ease of use
- Supports cold and warm restarts
  - Partition level
  - Module level
- Partition and module health management configuration uses XML
  - Developers can easily add their own custom HM handlers

Wind River VxWorks 653 Platform 2.4

Programming Environment

- Eclipse 3.8 platform
- Wind River GNU C, C++ compiler
- Multiple partition OS supporting:
  - ARINC 653 APEX API
  - VxWorks API subset
  - POSIX® API subset
- Analysis tools
  - System Viewer
  - Source code analyzer
- XML Configuration Suite
- Wind River Simics
  - System simulation tool



Wind River Workbench 3.3.6

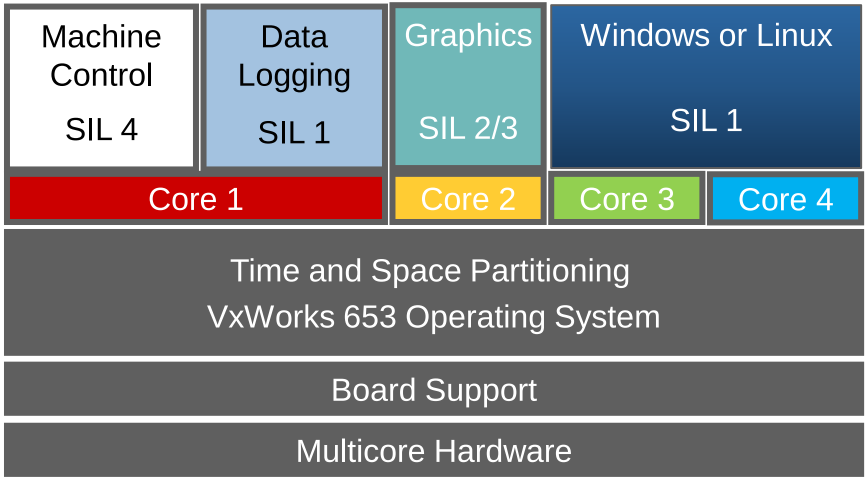
VxWorks 653

ControlSafe Hardware

Professional Services, Customer Support, Customer Education

Next Generation Supports Multi-core

- Multicore will come!
- Introduces more complexity to safety
  - Non-determinism
  - Resource interference
- Allows for many different software configurations
  - SMP
  - AMP
  - Mixed
  - Safety/non-safety



Machine Control

SIL 4

Data Logging

SIL 1

Graphics

SIL 2/3

Windows or Linux

SIL 1

Core 1

Core 2

Core 3

Core 4

Time and Space Partitioning

VxWorks 653 Operating System

Board Support

Multicore Hardware

Summary

- Wind River and Artesyn → Market Leaders in Their Fields
- ControlSafe Platform → SIL 4-Certified Railway Platform
- VxWorks 653 Operating System → Proven Partitioned Safety OS
- Future Systems → Multi-core and Virtualized