ControlSafe™ Expansion Box Platform

SIL4 COTS Fail-Safe and Fault-Tolerant System for Train Control and Rail Signaling Applications

DATA SHEET

- Highly integrated COTS safety platform certified to SIL4 by TÜV SÜD
- Cost-effective, common platform to enable various wayside applications
- High I/O capacity with larger chassis and I/O modules
- Designed to deliver platform hardware availability of six nines (99.9999%)
- A modular and scalable solution suitable for both new deployments and upgrade projects
- Innovative data lock-step architecture allows seamless technology upgrades
- Hardware-based voting mechanism maximizes application software transparency
- Rugged design compliant with IEC 61373 and EN 50155
- 15 years product life and 25 years of service available
- Backed up by a global service organization

Leveraging over 30 years of expertise in developing highly reliable and available embedded computer systems, SMART Embedded Computing is a premier supplier of commercial off-the-shelf (COTS) fail-safe computer systems to rail system integrators and rail application providers.

Certified to the highest safety level – SIL4 – by TÜV SÜD, one of the most trusted certification bodies worldwide, the ControlSafe™ Expansion Box Platform significantly enhances the growing SMART EC ControlSafe product portfolio. By leveraging the same safety architecture and technologies as the ControlSafe Platform, the cornerstone platform in the portfolio, the ControlSafe Expansion Box Platform is a highly integrated and cost-effective solution mainly targeting wayside applications such as Computer Based Interlocking (CBI) with its design of a larger chassis housing larger I/O modules.

As the worldwide investment in the rail infrastructure keeps rolling with a strong momentum, the networks of rail transportation have been ever expanding and becoming more and more complex. Addressing this challenge requires not only safer and smarter train control and rail signaling solutions, but also higher I/O capacities to handle the increasing data throughput. The ControlSafe Expansion Box Platform enables rail system integrators and rail application providers to integrate up to ten (10) 9U expansion I/O modules (EIOU) and one (1) 4U I/O module (xIOU) in a single chassis. By accommodating a variety of I/O types and allowing more ports and channels on each I/O module, this improved I/O processing capability can effectively reduce the number of chassis required to construct large scale applications.

Fully certified to EN 50126 for reliability, availability, maintainability and safety (RAMS) processes; EN 50128 for safety-related software; and EN50129 for safety-related electronic systems, SMART EC's ControlSafe Expansion Box Platform provides a cost-effective and application-ready safety platform for implementation in a SIL4 application environment. As opposed to designing and building one from scratch, adopting the ControlSafe Expansion Box Platform as the core safety processing engine enables rail application developers and system integrators to effectively reduce cost and risk by leveraging a SIL4 COTS platform, and substantially accelerate time-to-market by focusing on their value-added offering and final certification for the end solutions.

CONTROL SAFE™

SMART™ Embedded Computing

ControlSafe Expansion Box Platform Data Sheet

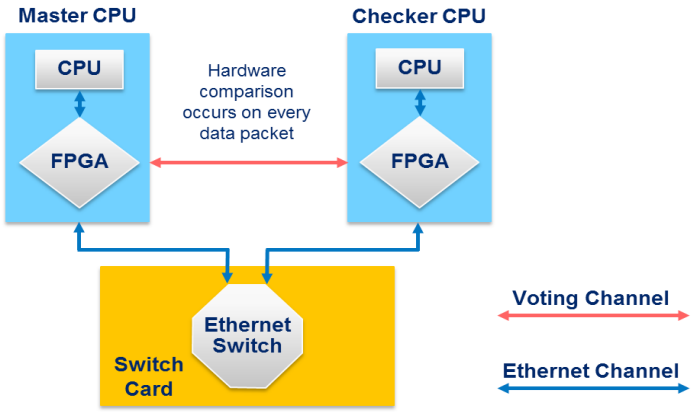
The shared safety architecture, featuring innovative data lock-step and hardware based voting, makes it easy to transfer applications between the ControlSafe Expansion Box Platform and the ControlSafe Platform. This further bolsters SMART EC's design philosophy by delivering a "Common Platform" to enable various applications and therefore help customers maximize the return on investment. In addition, the ControlSafe Expansion Box Platform can also be deployed as an I/O expansion subsystem to meet specific application requirements.

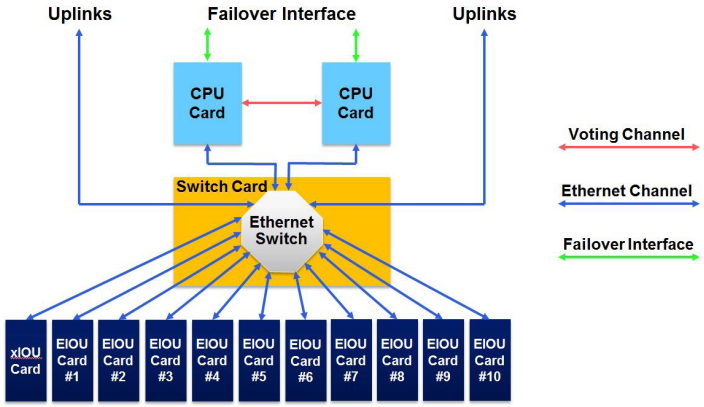
SMART EC is committed to building long-term partnerships with customers, based on proven and reliable systems with consistent performance. The ControlSafe Expansion Box Platform further strengthens this commitment by providing rail industry customers with an unmatched, highly reliable platform with 15 years of planned product life and 25 years of extended support and service available.

Adhering to SMART EC's future-proof development philosophy, the ControlSafe Expansion Box Platform is modular, scalable and designed to seamlessly accommodate additional I/O interfaces as well as upgraded processors throughout the product life cycle. SMART EC is focused on continued platform development to build a comprehensive product line to enable customers to seamlessly integrate the ControlSafe Expansion Box Platform in a variety of rail signaling applications. SMART EC's ultimate goal is to enhance customers' competitive position by allowing them to focus their development efforts on differentiating end applications.

CONTROLSAFE EXPANSION BOX ARCHITECTURE

At the core of each Expansion Box (EXB) are two identical CPU boards that run in data lockstep mode and implement a two-out-of-two (2oo2) voting mechanism. In the data lockstep mode, a deterministic boundary is created at the data fabric interface of the two CPUs. All transactions that are about to cross this deterministic boundary are compared to confirm correct operation of the two CPUs. As opposed to a hard lockstep mode, where the processor clocks are synchronized and the deterministic boundary is created at the address and data buses of the processors, the data lockstep mode can be implemented using modern high-performance processors which are not viable options for a hard lockstep safety architecture.





Comparison of the data fabric bound transactions is done using a 2oo2 voting mechanism, where any discrepancy between these two CPUs is considered a failure and causes the EXB to enter a fail-safe mode. In the fail-safe mode, by default all output ports are driven to their safe/silent state, eliminating any possibility of setting external equipment to a wrong state.

The EXB's data lock-step architecture makes it possible to upgrade the processor architecture over time while retaining the same I/O. Having implemented the 2oo2 voting facilities in hardware allows application developers to migrate existing application software with minimal modifications.

Targeting mainly wayside applications, the SMART EC ControlSafe Expansion Box Platform is designed to support a broad range of I/O modules such as CAN, Ethernet, Ethernet Ring, UART, digital and analog to enable solution integrators to handle both new deployments and upgrade projects easily. All communication I/O modules have a common architecture based on the same NXP® CPU and the same Wind River VxWorks 653 operating system, thus simplifying the software development environment. All I/O modules are accessed over Ethernet allowing a seamless distributed programming model. All modules support remote on-line software and firmware upgrade without risk of rendering a system inoperable. All I/O ports are user programmable as safety-relevant or non-safety relevant. In addition, the Switch Module provides three (3) 10/100/1000Base-T ports via its rear transition module (RTM), for direct Ethernet/IP access to other processing nodes in the application's network or to the peer EXB.

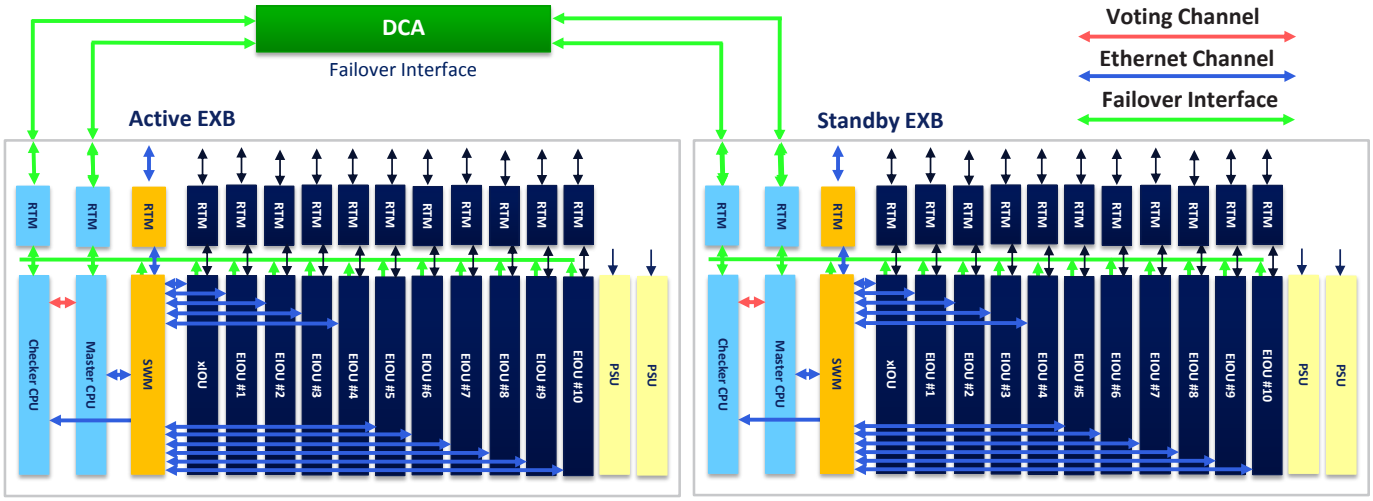
Chassis-Level Fault Management

The SMART EC ControlSafe Expansion Box Platform provides chassis-level Fault Management capabilities, utilizing both run time and in line diagnostics. Each Module runs a strenuous diagnostic check on start up (POST) to ensure readiness. A hardware-based Health and Safety monitoring subsystem connects to all modules in a chassis, including I/O modules. Hardware-based in line diagnostics provide continuous checking for latent faults in Safety Functions through the entire Safety path of the chassis, and Software Run Time Diagnostics provide checking of the correct operation of diagnostic functions. Hardware-detected, safety-related faults cause an immediate transition of all Safety Functions to the Failsafe state.

ControlSafe
Expansion Box
Platform
Data Sheet

CONTROLSAFE EXPANSION BOX PLATFORM ARCHITECTURE

SMART EC's ControlSafe Expansion Box Platform consists of two redundant EXBs, each of which delivers fail-safe operations and together provide a highly available platform. They are linked by a Direct Connect Algorithm (DCA) that monitors the health of the two EXBs and designates one of them as 'active' and the other as 'standby'. The user application running on the active EXB has full control of all I/O. The same user application running on the standby EXB can monitor safety-relevant input, but by default has no ability to drive any safety-relevant output. When the active EXB fails, its safety-relevant output is suppressed and it signals its state through the DCA, which in turn causes the standby EXB to become active and begin driving its safety-relevant output. The unhealthy EXB is taken out of operation and, once it has been repaired by service personnel, can be brought back into service. Monitoring the health state of the two EXBs and controlling fail-over operation between them provides a highly available fail-safe computing system.



ACTIVE/STANDBY CONTROL

SMART EC's ControlSafe Expansion Box Platform supports Active/Standby control with the Direct Connect cabling method.

Direct Connect

The Direct Connect method uses a patented algorithm and special cables to link the two EXBs. Health status is exchanged and tracked in state machines running on all the CPU modules to control the active and standby roles. When power is applied, the first EXB that has healthy signals from both CPUs goes active. The Direct Connect Algorithm (DCA) is designed so that only one EXB can be active at a time, and that only a healthy EXB can be active.

POWER SUBSYSTEM

The EXB includes redundant (1+1) AC Power Supply FRUs (PSU). Either is capable of powering a fully populated EXB. If one PSU fails, the other provides power to ensure continuous operation. Software can monitor the health of the PSUs.

COOLING SUBSYSTEM

A Fan Tray FRU is included that provides autonomous operation. When the ambient inlet temperature reaches a set temperature, the fan tray turns on. The fans ramp up to full speed at approximately 55 °C. Software can monitor the health and operational status of the fan tray. The fan tray can provide sufficient cooling with any single fan failure.

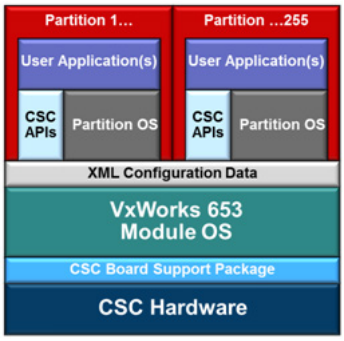
EIOU DEVELOPMENT

The ControlSafe Expansion Box Platform is designed as a common base platform to enable various applications through the continuous addition of SMART EC EIOU modules. In addition, SMART EC offers customers the flexibility to develop EIOU modules and I/O backplanes to meet their specific needs by providing all necessary technical specifications, product support and service. The business model is intended to enhance the collaboration between SMART EC and customers and enable them to utilize available resources effectively and efficiently to handle both new development and upgrade projects.

ControlSafe
Expansion Box
Platform
Data Sheet

OPERATING SYSTEM

All modules in the ControlSafe Platform support Wind River's VxWorks 653 operating system. It provides both resource management and a partitioning environment that permits multiple independent applications of different criticality levels to run on a single target platform under protected conditions. At the heart of VxWorks 653 is the Core OS. The Core OS component uses the features of the target architecture to enforce isolation between applications residing in separate partitions. The partitions can contain application software that is supported by one of three interface layers: VxWorks-based APIs, APEX Interface (ARINC 653 Interface), or POSIX APIs. These interface layers provide various levels of scheduling and thread management to the application. In addition to controlling partition memory and CPU time usage, the Core OS also provides services to manage system resources, such as I/O.



The Core OS implements a partition scheduler using a statically defined configuration table that allocates CPU cycles to each partition and specifies the order of partition execution. The Core OS manages all shared resources on behalf of the application partitions including system time and memory. The Core OS ensures that resources required by an application partition are available to it after a partition switch, and prevents applications from corrupting each other. Communications between partitions, and between partitions and the Core OS, are only performed if appropriate communication channels are used, and if they are permitted by the system configuration table.

The VxWorks 653 Health Monitor (HM) provides a framework to raise and handle events such as alarms or messages in an Integrated Modular Avionics (IMA) system. The framework supports the ARINC API, and includes a standalone API. The HM functions at three levels: module, partition and process. Fault responses and recovery actions are table-driven at the partition and module level, while application actions are driven at the process level. Partition or module level handlers can communicate information to other partitions by notifying them of given events. For instance, one partition handler can tell another about an event that caused it to restart the partition.

APPLICATION PROGRAMMING INTERFACES

A library of Application Programming Interfaces (APIs) is provided to ease the process of building a safety application. These provide functions that can query the state of the safety logic, aid with the communications between the layers and monitor health of vital components like the system memory. In addition there are a range of control and status APIs giving the safety application full control down to the level of watchdog timer, I/O port control and physical health monitoring. The following is the list of APIs:

- Control/Status
- DRAM Scrubber
- Firmware Upgrade
- Flash Integrity
- Link Health Check
- Logging
- Maintenance Mode Watchdog
- Network Routing
- Persistent DRAM
- Platform Management
- Runtime Diagnostics
- Switch Management
- Safety Layer
- Vital Product Data (VPD)
- Voting Logic

CERTIFICATION EVIDENCE

SMART EC's ControlSafe Expansion Box Platform strictly adheres to all industry specifications and standards required to deliver a highly reliable and available platform for modern safety applications. SMART EC provides customers with a complete Certification Evidence Package to facilitate the certification process for their integrated systems.

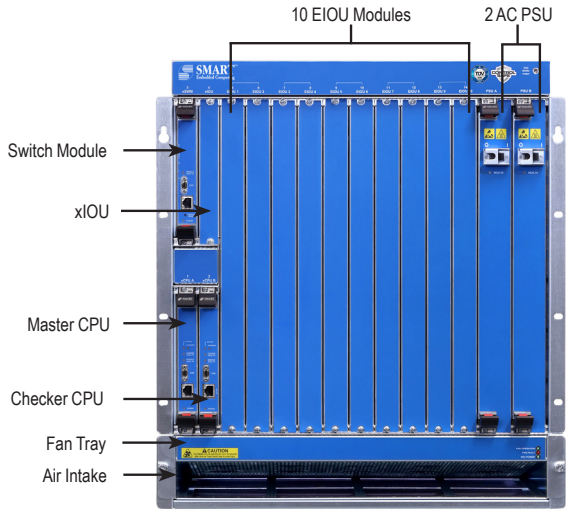
The Certification Evidence Package includes:

- Safety Case
  - Definition of system
  - Quality management report
  - Safety management report
  - Technical safety report
- Safety Assessment Report
- Safety Manual
  - Specifies user's actions required to enable the integration of SMART EC's ControlSafe Expansion Box Platform into a safety-relevant system
- Safety certificate *No. Z10 16 10 87324 011* issued by TÜV SÜD

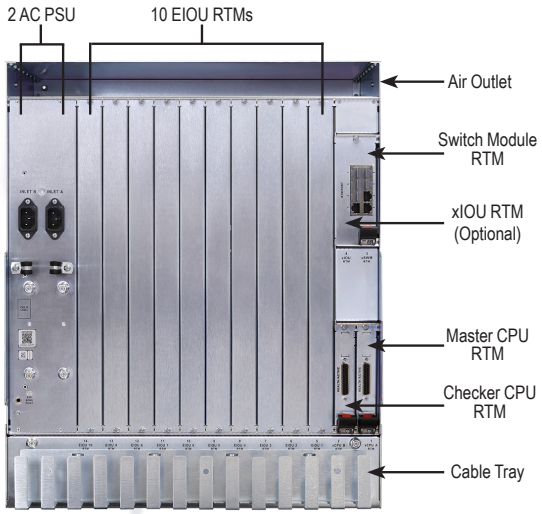
ControlSafe
Expansion Box
Platform
Data Sheet

SYSTEM CHASSIS

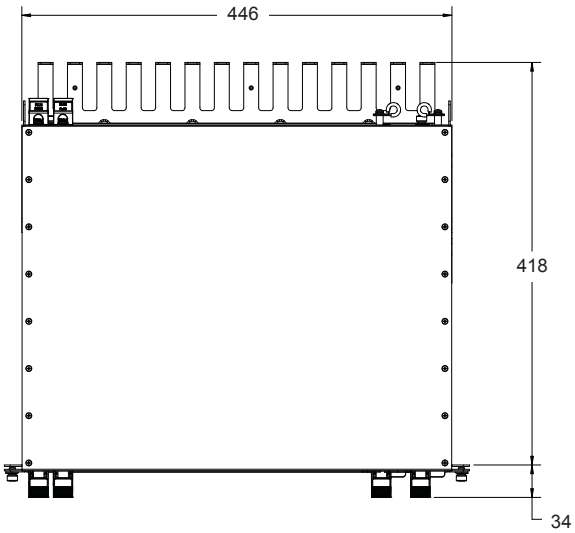
Front View

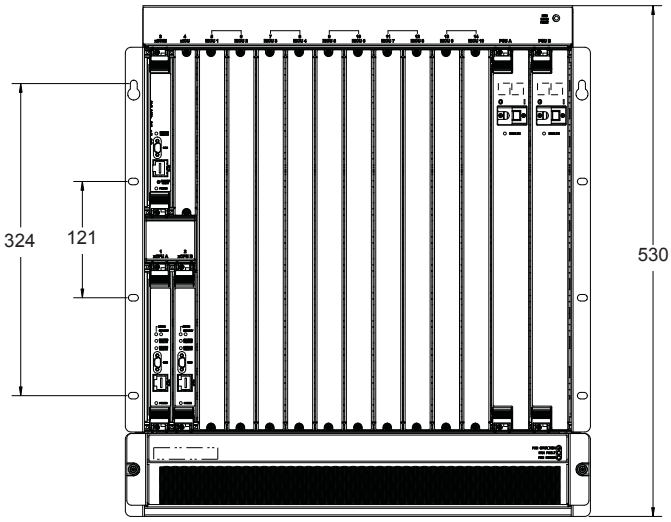


Rear View

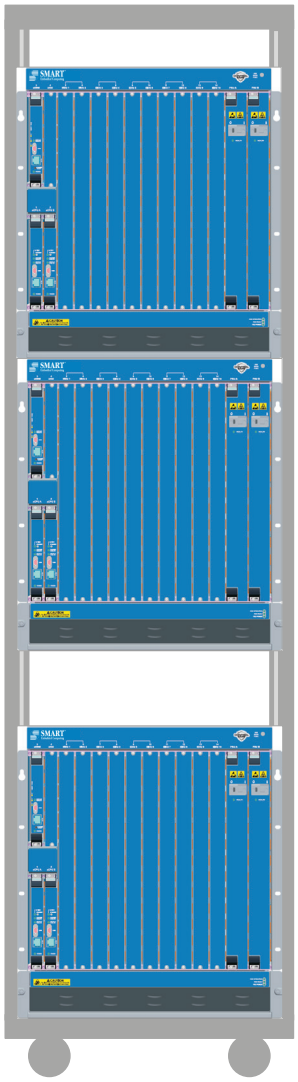


EXB DIMENSIONS (UNIT: MM)





SYSTEM RACK MOUNTING EXAMPLES



ControlSafe Expansion Box Platform Data Sheet

Technical Specifications

	Processor Modules	Switch Module and xIOU Modules
Processor	NXP P2020 (1 GHz)	NXP P1011 (800 MHz)
Operating System	VxWorks 653	VxWorks 653
Memory	1GB (optional 4GB) DDR3-800 SDRAM, ECC	512MB (optional 2GB) DDR3-667 SDRAM, ECC
Flash	2 X 128MB NOR	2 X 64MB NOR
MRAM	2 X 2MB MRAM	1 X 2MB MRAM
Front Panel Maintenance Ports	10/100/1000 BASE-T and RS-232	10/100/1000 BASE-T and RS-232 (Switch Module only)
Data Fabric	Fourteen (14) GbE links	
Board Management	Voltage and temperature sensors	

I/O Interfaces	
Number of IOU Slots	Ten (10) 9U Expansion IOU (EIOU); One 4U (1) xIOU
10/100/1000 BASE-T Ethernet Ports	Standard: Three (3) from Switch Module

Physical Specifications	
Operating Temperature	-40 °C to 70 °C
Cooling	Forced Air and Convection cooled
Power	AC: 90-264V, 47-63Hz
Vibration	Compliant with EN 61373, Category 1, Class B (EN 50155 12.2.11)
Shock	Compliant with EN 61373, Category 1, Class B (IEC 60068-2-27)
Chassis Sealing	Standard: IP20; Optional: IP30
Conformal Coating	ST1 rating for EN 50155 Section 12.2.10 (Salt Mist Test)
Standards	Designed in accordance with EN50121, EN50124, EN50155, EN50126, EN50128, EN50129, EN55024, EN60529, EN60571, IEC61508. See documentation for specific compliances.
Safety Certificates	EN50126, EN 50128, EN50129 (SIL4) and IEC61508 (SIL3) (Safety Certificate No. Z10 110176 0001 issued by TÜV SÜD)

Ordering Information	
Part Number	Description
CSP-EXB-CORE-AC-01	ControlSafe Expansion Box Platform core that comprises one chassis, two AC power supply units, two CPU modules, one switch module and one fan tray
CSP-EXB-FILL-01	4U Front filler panel
CSP-EXB-FILL-02	9U Front filler panel
CSP-EXB-FLL-RTM-01	3U Rear filler panel
CSP-EXB-FLL-RTM-02	9U Rear fillerpanel
CSP-CBL-DIRECT-01	Two cables for Direct Connect (DCA) operation
CSP-CBL-PWR-B-01	Power cord for USA/Canada/Japan
CSP-CBL-PWR-EU-01	Power cord for Korea/Germany/France
CSP-CBL-PWR-I-01	Power cord for China
SERIAL-MINI-D2	Serial cable - micro D-sub connector to standard DE9

Note: The components of the ControlSafe Platform core are not listed in this table but can be ordered separately as spare parts.
Please contact SMART EC regional sales teams for further details.

SOLUTION SERVICES

Smart Embedded Computing provides a portfolio of solution services optimized to meet your needs throughout the product lifecycle. Design services help speed time-to-market. Deployment services include worldwide technical support. Renewal services enable product longevity and technology refresh.

CONTACT DETAILS

+1 602-438-5720
Info@smartembedded.com
www.smartembedded.com/ec/contact

SMART™ Embedded Computing