ControlSafe™ Carborne 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
- Compact, versatile platform suitable for both carborne and wayside applications
- Common ControlSafe safety architecture boosts flexibility of solution selection
- Designed to deliver platform hardware availability of six nines (99.9999%)
- A modular and scalable solution enables 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 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™ Carborne 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, and ControlSafe Expansion Box Platform, the ControlSafe Carborne Platform is a highly integrated and cost-effective solution mainly targeting onboard applications such as Automatic Train Protection (ATP), Automatic Train Operation (ATO), and Positive Train Control (PTC) with its design of a compact 4U chassis, front access I/O and DC power supply.

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 complex. Trains run faster and are dispatched at a higher frequency with a shorter headway, and in addition, the advancement of wireless communication technologies accelerates the migration of certain processing functions from wayside equipment to carborne systems. Addressing these technical challenge requires not only safer, smarter and more rugged carborne signaling and control solutions, but also higher I/O capacities to handle the increasing data throughput and a broad range of I/O interfaces. SMART EC's ControlSafe Carborne Platform allows rail system integrators and rail application providers to integrate up to twelve (12) I/O modules in a single chassis. By harnessing a strong processing power and accommodating a variety of I/O types, this platform enables customers to either handle upgrade projects smoothly or take on green-field projects effectively.

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 Carborne 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 Carborne 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.

SMART™ Embedded Computing

The shared safety architecture, featuring innovative data lock-step and hardware based voting, makes it easy to transfer applications between the ControlSafe Carborne Platform, ControlSafe Platform and ControlSafe Expansion Box 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. The lineup of SMART EC's three platforms provides a great level of flexibility allowing customers to choose the solution that best meets their needs.

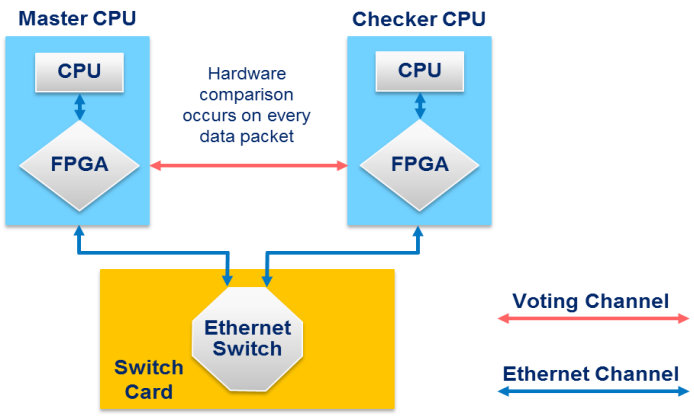
SMART EC is committed to building long-term partnerships with customers, based on proven and reliable systems with consistent performance. The ControlSafe Carborne Platform further strengthens this commitment by providing rail industry customers with an unmatched, highly reliable platform with 15 years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

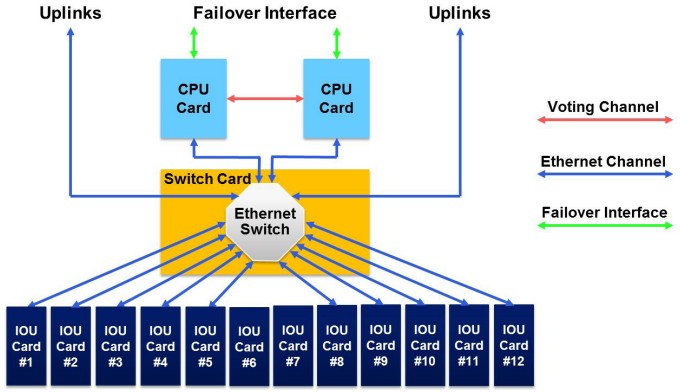
Adhering to SMART EC's future-proof development philosophy, the ControlSafe Carborne Platform is modular, scalable and designed to seamlessly accommodate additional I/O interfaces as well as upgraded processors throughout the product life cycle.

SMART EC is focused on continued platform development to build a comprehensive product line to enable customers to seamlessly integrate the ControlSafe Carborne 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 CARBORNE COMPUTER ARCHITECTURE

At the core of each ControlSafe Carborne Computer (CCC) 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.





For the current implementation, I/O slot #6 and #7 are not connected on the data fabric and only for external I/O aggregation; slot #12 is reserved for SMART EC's CAN I/O module.

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 CCC 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 CCC'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.

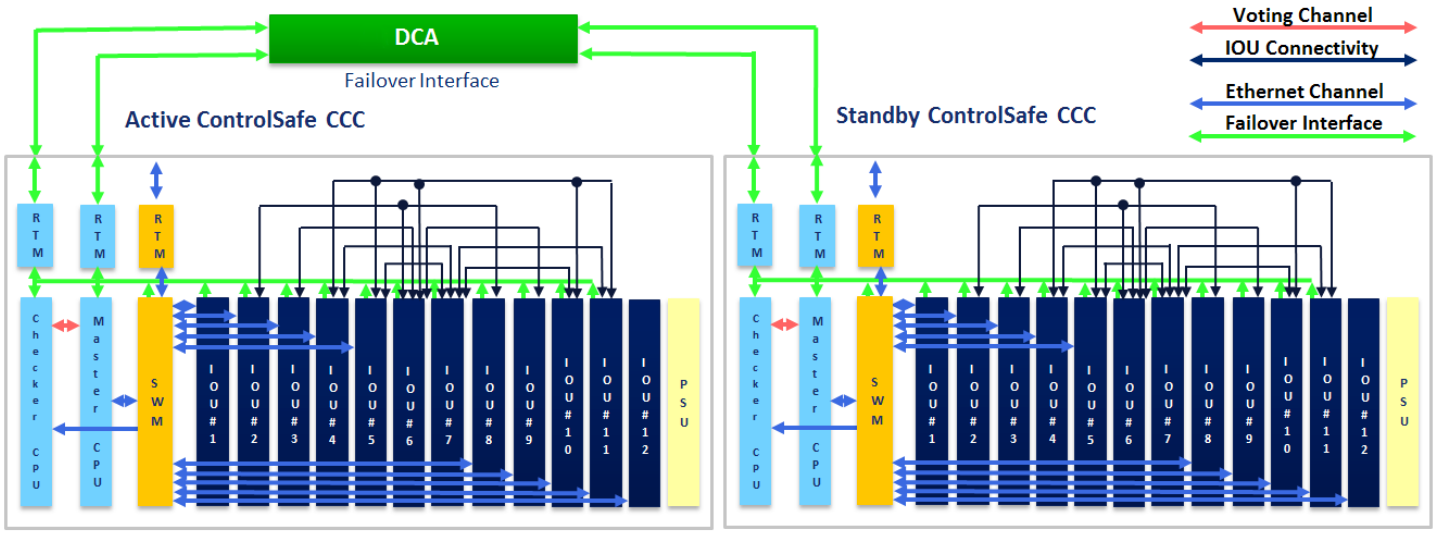
Targeting mainly carborne applications, the SMART EC ControlSafe Carborne Platform is designed to support a broad range of I/O modules such as CAN, Ethernet, Ethernet Ring, MVB, GPS/Wireless, UART, digital and analog to enable solution integrators to easily handle a wide spectrum of deployments. All intelligent 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 four (4) 10/100/1000Base-T ports with rugged M12 connectors via its rear transition module (RTM), for direct Ethernet/IP access to other processing nodes in the application's network or to the peer CCC.

Chassis-Level Fault Management

The SMART EC ControlSafe Carborne Platform provides chassis-level Fault Management capabilities, utilizing both run time and in line diagnostics. Each Module runs a strenuous diagnostic check on startup (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 Fail-safe state.

CONTROLSAFE CARBORNE PLATFORM ARCHITECTURE

SMART EC's ControlSafe Carborne Platform consists of two redundant CCCs, 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 CCCs and designates one of them as 'active' and the other as 'standby'. The user application running on the active CCC has full control of all I/O. The same user application running on the standby CCC can monitor safety-relevant input, but by default has no ability to drive any safety-relevant output. When the active CCC fails, its safety-relevant output is suppressed and it signals its state through the DCA, which in turn causes the standby CCC to become active and begin driving its safety-relevant output. The unhealthy CCC 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 CCCs and controlling fail-over operation between them provides a highly available fail-safe computing system.



ACTIVE/STANDBY CONTROL

SMART EC's ControlSafe Carborne 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 CCCs. 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 CCC that has healthy signals from both CPUs goes active. The Direct Connect Algorithm (DCA) is designed so that only one CCC can be active at a time, and that only a healthy CCC can be active

I/O MODULE DEVELOPMENT

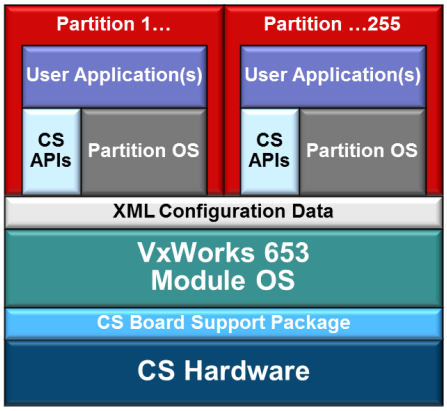
The ControlSafe Carborne Platform is designed as a common base platform to enable various applications through the continuous addition of SMART EC IOU modules. In addition, SMART EC offers customers the flexibility to develop IOU modules and specify I/O backplane connectivity to meet their specific needs 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 projects with varying levels of requirements.

OPTIONAL INTEGRATED FAN COOLING SUBSYSTEM

In order to enable customers to address various operating environments, SMART EC also offers an optional integrated fan cooling subsystem to ensure that a fully populated and fully operational ControlSafe Carborne Platform chassis operates from -40 °C to +70 °C inlet ambient temperature. The active air cooling subsystem consists of an installation bay fixed at the bottom of the chassis and a 1U hot pluggable, modular and autonomous fan tray that only activates if the inlet ambient temperature exceeds a minimum threshold temperature. The fan tray can provide sufficient cooling with any single fan failure. When the cooling system is in operation, air flow is bottom-to-top. Featuring a controller, the fan tray operation status is indicated by front panel LEDs and can be polled by the ControlSafe Carborne Platform over an I²C interface.

OPERATING SYSTEM

The ControlSafe Carborne Platform supports Wind River's VxWorks 653 operating system and programming environment for user programmable modules, specifically the CPU, SWM, and CAN. VxWorks 653 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.



**CS - ControlSafe*

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 Carborne 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.

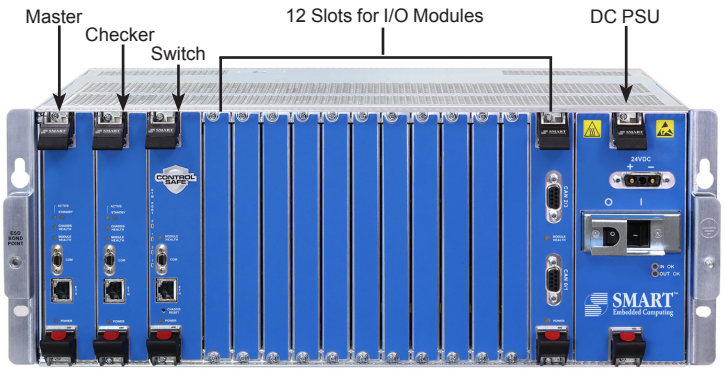
The Certification Evidence Package includes:

- 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 Carborne Platform into a safety-relevant system
- Safety certificate *No. Z10 17 09 87324 012* issued by TÜV SÜD

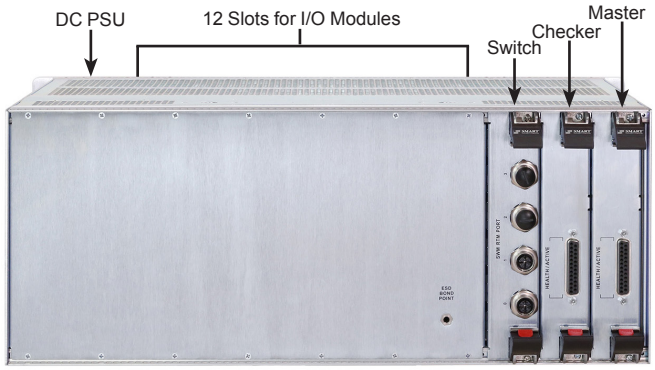
ControlSafe
Carborne Platform
Data Sheet

SYSTEM CHASSIS

Front View

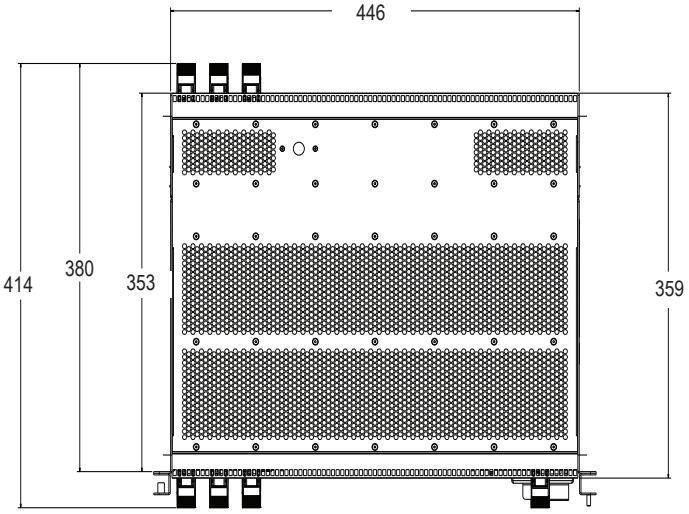


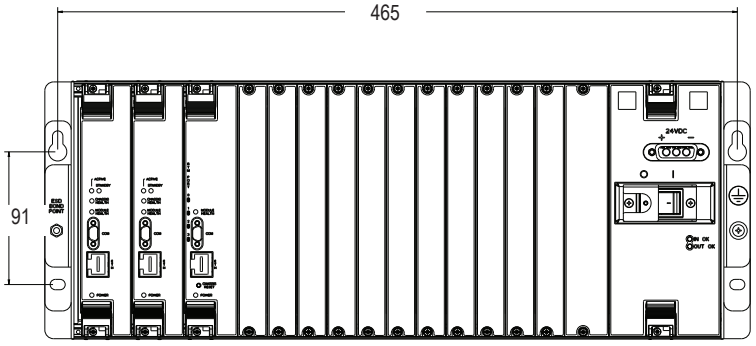
Rear View



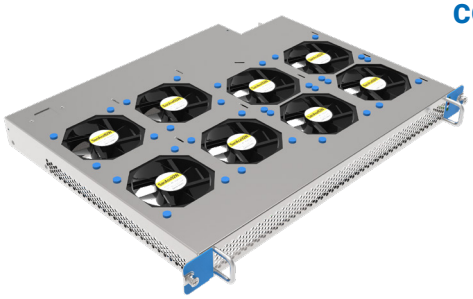
CONTROLSAFE CARBORNE COMPUTER DIMENSIONS

Units in mm

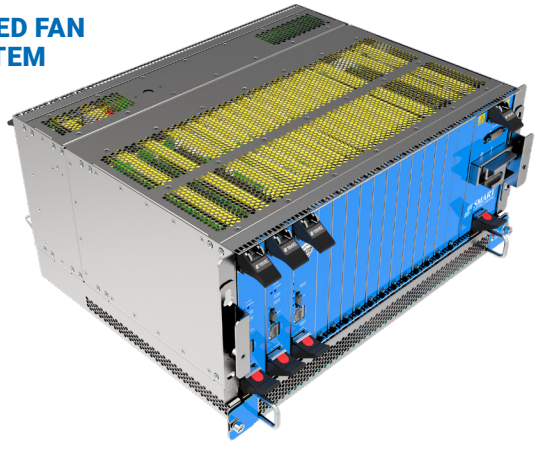




OPTIONAL INTEGRATED FAN COOLING SUBSYSTEM



Fan Tray



CCC Chassis with Fan Tray Installation Bay

ControlSafe
Carborne Platform
Data Sheet

Technical Specifications

	Processor Modules	Switch Module and CAN IOU Module	UART and Digital IOU Modules
Processor	NXP P2020 (1 GHz)	NXP P10110 (800 MHz)	Altera Cyclone V SoC and FPGAs
Operating System	VxWorks 653	VxWorks 653	Linux (not user-programmable)
Memory	1GB (optional 4GB) DDR3-800 SDRAM, ECC	512MB (optional 2GB) DDR3-667 SDRAM, ECC	512MB DDR3-800 SDRAM, ECC
Flash	2 X 128MB NOR	2 X 64MB NOR	2 X 64MB NOR
MRAM	2 X 2MB MRAM	1 X 2MB MRAM	1 X 512KB MRAM
Maintenance Ports	10/100/1000 BASE-T and RS-232	10/100/1000 BASE-T and RS-232 (Switch Module only)	RS-232
Data Fabric	Thirteen (13) GbE links		
Board Management	Voltage and temperature sensors		

I/O Interfaces	
Number of IOU Slots	Twelve (12)
10/100/1000 BASE-T Ethernet Ports	Standard: Four (4) from Switch Module
CANbus Ports	Optional: Four (4) per CAN IOU
Serial UART	Optional: Eight (8) per UART IOU
Digital Inputs	Optional: Sixteen (16) per Digital Input IOU
Digital Outputs	Optional: Eight (8) per Digital Output IOU

Physical Specifications		
Operating Temperature	-40 °C to 50 °C	in open rack environment
	-40 °C to 70 °C	in a closed rack installation with a required airflow measured at the intake to the bottom of chassis; or with an optional integrated fan cooling solution
Cooling	Forced Air and Convection Cooled	
Power	DC: 24V	
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 0002 issued by TÜV SÜD)	

Ordering Information	
Part Number	**Description**
CSP-CCC-CORE-DC-01	4U ControlSafe Carborne Computer core that comprises of one chassis, one DC PSU, two CPU modules, and one switch module
CSP-CCC-CORE-DC-02	4U ControlSafe Carborne Computer core that comprises of one chassis, one DC PSU, two CPU modules, one switch module, and one 1U budget fan cooling system
CSP-CCC-CORE-DC-03	4U ControlSafe Carborne Computer core that comprises of one chassis, one DC PSU, two CPU modules, one switch module, and one 1U premium fan cooling system
CSP-CCC-CAN-01	4-port CAN I/O module
CSP-CCC-UART-01	8-port UART I/O module
CSP-CCC-CHS-FAN-02	Budget replacement fan tray FRU
CSP-CCC-CHS-FAN-03	Premium replacement fan tray FRU
CSP-CCC-FAN-BAY-01	1U bay installation kit for fan tray FRU
CSP-CCC-FILL-01	4HP filler panel
CSP-CCC-BAY-FLL-01	Filler panel for bay installation kit
CSP-CBL-DIRECT-01	Two cables for Direct Connect (DCA) operation
SERIAL-MINI-D2	Serial cable - micro D-sub connector to standard DE9

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