COMPUTING

ControlSafe® 紧凑型车载平台

致力于列车运行控制和铁路信号应用的 SIL4 级别商业成品 (COTS) 故障安全容错系统

数据表

- 高度集成的 COTS 安全平台，设计为符合 SIL4 认证
- 封装尺寸小巧 (44HP)，可在标准 19”机架中并排安装两个机箱
- 紧凑的表决和处理引擎提升了终端解决方案的灵活性和模块化程度
- 多功能平台，适用于车载和轨旁应用
- 通用 ControlSafe 安全架构将转移应用的工作量降至最低
- 设计用于实现一流的平台硬件可用性（高达 99.9999%）
- 模块化且可扩展的解决方案，新增部署和升级项目皆适用
- 创新的数据同步架构，助于实现系统的无缝技术升级
- 以硬件为基础的安全表决机制，有效提高应用软件的透明度和可移植性
- 符合 IEC 61373 和 EN 50155 标准的加固强化设计
- 生命周期长达 15 年，且可享受 25 年的超长支持和服务
- 全球性服务机构鼎力支持

凭借 30 多年来在高可靠和高可用性嵌入式计算系统领域的专业开发经验，雅特生科技早已跻身于全球领先的安全容错系统供应商行列。如今，我们正致力于为铁路系统集成商和铁路信号控制应用开发企业设计和制造最先进的，面向未来的下一代安全计算平台。

作为标准 ControlSafe® 车载平台的衍生平台，ControlSafe® 紧凑型车载平台通过了最高安全级别 SIL4 的认证，为不断壮大的雅特生科技 ControlSafe 产品组合打造坚固后盾。ControlSafe 紧凑型车载平台沿用与作为该产品组合基础平台的 ControlSafe 安全平台和 ControlSafe Expansion Box 平台相同的安全架构和技术，是一款高度集成且极具成本效益的解决方案。平台采用宽度仅为半个机架的紧凑型 4U 机箱、前面板输入/输出访问和直流电源设计，主要针对列车自动保护系统 (ATP)、列车自动运行系统 (ATO) 和列车主动控制系统 (PTC) 等板载应用。

对比标准 ControlSafe 车载平台，紧凑型平台保留加工和表决功能所需的相同“核心”的同时，还将输入/输出插槽的数量从 12 个缩减至 1 个。新型结构将机箱宽度减少 50%，因此能在标准 19” 机架中并排安装两个平台机箱。得益于小巧的尺寸，雅特生科技的 ControlSafe 紧凑型车载平台确保集成商能够在十分有限的安装空间内高效解决极富挑战性的应用。更为重要的是，ControlSafe 紧凑型车载平台作为连接并驱动专用外部输入/输出盒和设备的加工和表决引擎，提升了终端解决方案的灵活性和模块化程度。该设计有助于集成商通过 ControlSafe 紧凑型车载平台仅升级安全体系的“核心”，从而为其投资现有输入/输出模块提供保障。

雅特生科技 ControlSafe 紧凑型车载平台在可靠性、可用性、可维护性和安全性 (RAMS) 方面全面通过了 EN 50126 认证，其安全相关软件通过了 EN 50128 认证，安全相关电子系统则通过了 EN50129 认证，是一款极具成本效益且应用就绪的安全平台，适用于 SIL4 级别的应用环境。相较于从零开始设计和构建，采用 ControlSafe 紧凑型车载平台作为核心安全处理引擎将有利于铁路应用开发企业和系统集成商充分利用 SIL4 级别商业现货平台来有效降低成本和风险，使其能专注于为终端解决方案提供增值产品和最终认证，从而大幅缩短产品的研发和上市周期。

CONTROL SAFE™

ARTESYN™
EMBEDDED TECHNOLOGIES

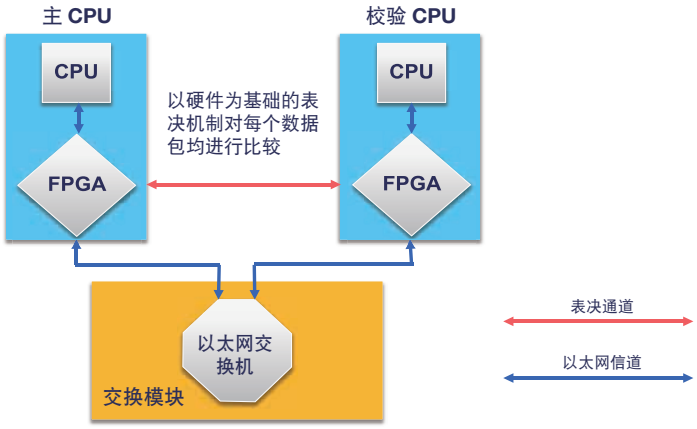
共享安全架构采用创新的数据同步和基于硬件的表决，可在 ControlSafe 紧凑型车载平台、ControlSafe 平台和 ControlSafe Expansion Box 平台，以及标准 ControlSafe 车载平台之间轻松转移应用。这样打造出来的“通用平台”，可实现各种应用，并最大程度地提高客户的投资回报，将雅特生科技的设计理念发扬光大。雅特生科技的三大平台组合提供了更高程度的灵活性，使客户能够选择最适合自己需要的解决方案。

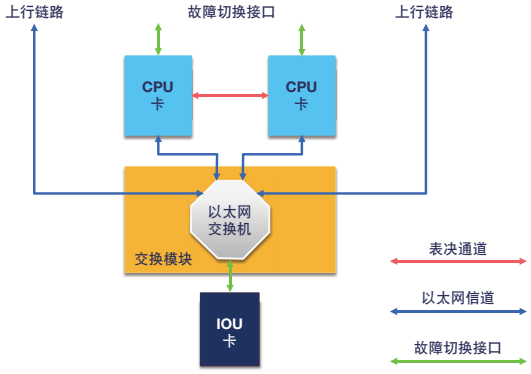
以科技为本造就基业长青，雅特生科技依靠久经实际应用检验且稳定可靠的产品来赢取与客户间的长期合作与信赖。ControlSafe 紧凑型车载平台的推出更进一步体现了雅特生科技对此信念的执着。正是本着对铁路行业在产品生命周期上要求近乎苛刻的深刻理解，雅特生科技的 ControlSafe 车载平台以领先行业的高可靠性为客户提供长达 15 年的产品寿命以及 25 年的技术支持和维护服务，这将成为客户投资回报最大化的有力保障。模块化且可扩展的 ControlSafe 紧凑型车载平台秉承雅特生科技面向未来的开发理念，在整个产品生命周期中均可无缝容纳附加输入/输出接口和升级版处理器。

雅特生科技致力于持续的平台研发，以建立丰富完善的产品线，使得客户可以将 ControlSafe 紧凑型车载平台无缝集成到各种铁路信号应用中。雅特生科技的最终目标在于让客户能够专注于开发个性化的终端应用，从而提升客户的竞争地位。

CONTROLSAFE 紧凑型车载计算机构架

运行在每一台 ControlSafe 紧凑型车载计算机 (C-CCC) 里的核心组件是两片完全相同的 CPU 模块。ControlSafe 车载平台在数据同步模式下的二取二表决机制 (2oo2) 便由这两片 CPU 模块来执行。在数据同步模式下，表决的确定性边界创建在两片 CPU 模块的数据交换接口处。系统会将所有通过确定性边界的数据交换都进行比较，以确认两片 CPU 模块运行正常。在硬同步模式下，不同模块间的同步是通过处理器的时钟来实现的，而且表决的确定性边界创建于处理器的地址和数据总线；而在数据同步模式下，只需利用高性能的现代处理器即可实现，这对硬同步安全架构而言却不可行。





C-CCC 通过二取二表决机制进行数据交换的比较。在此机制下，一旦两片 CPU 模块出现运行处理不一致的状况，系统将即刻表决认定该 C-CCC 发生故障，并将其切换到故障安全模式。在故障安全模式的默认设置下，所有输出端口都将被设定为安全 / 非安全状态，从而避免系统因输出错误数据而导致对外部相关设备的不当控制。

C-CCC 采用数据同步架构，可确保客户在将来对处理器架构进行升级时仍能保留相同的输入/输出。除此之外，ControlSafe 安全平台基于硬件实现的二取二表决机制还将显著提高应用软件的透明度和可移植性，因此能帮助客户尽可能地减少移植现有应用软件时的修改工作，从而使客户获得对时间和资金成本控制的双重优势。

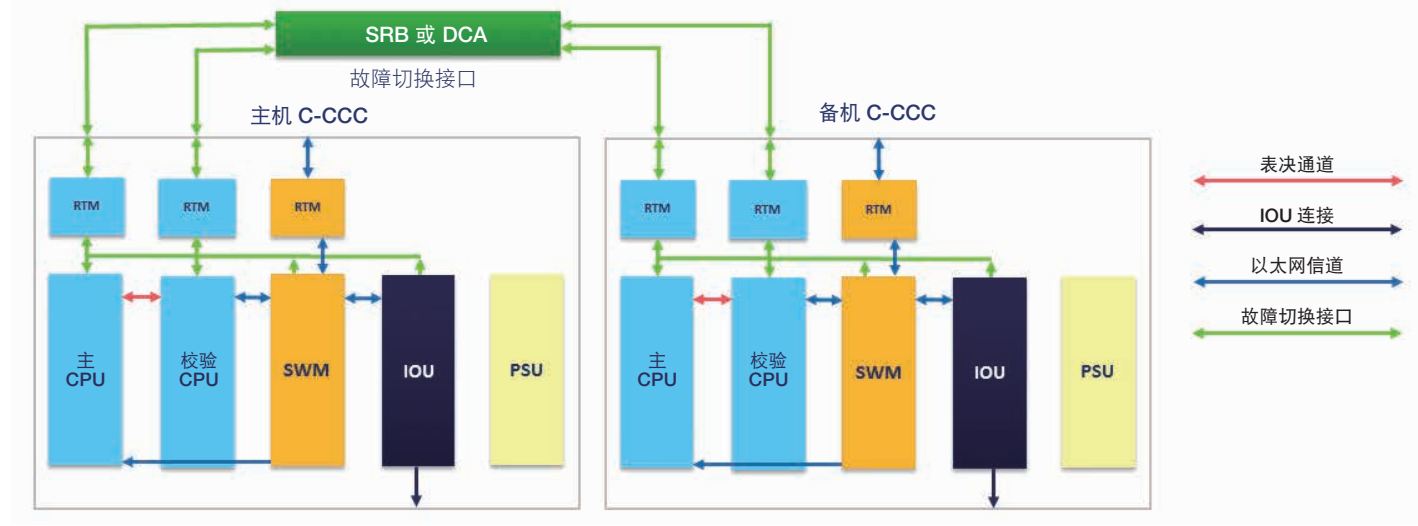
雅特生科技 ControlSafe 紧凑型车载平台主要设计用于车载应用，得益于标准车载平台研发的优势，可支持 CAN、以太网、以太网环网、MVB、GPS/无线、UART、数字和模拟等各类输入/输出模块，从而帮助解决方案集成商轻松进行各类部署。所有智能输入/输出模块均可通过以太网访问，从而实现无缝分布式编程模型。所有模块均支持远程联机软件和固件升级，不会导致系统无法使用。所有输入/输出端口均可由客户设计为与安全相关或与安全无关。此外，交换模块的后方转换模块 (RTM) 上提供了四 (4) 个带加固型 M12 连接器的 10/100/1000Base-T 端口，可用于通过以太网/IP 地址直接访问应用网络中的其他处理节点或者对等 C-CCC。

机箱级故障管理

雅特生科技的 ControlSafe 紧凑型车载平台具有机箱级故障管理性能，充分利用运行时间诊断和在线诊断两者。各模块在启动时进行繁复的诊断检查 (POST)，以确保其准备就绪。基于硬件安全监控子系统与机箱中的所有模块相连，包括输入/输出模块。硬件的在线诊断针对整个机箱安全路径范围内各安全功能中的潜伏性故障执行连续的检查，而软件运行时间诊断则检查诊断功能是否正确运行。硬件检测到安全相关故障时，所有安全功能即刻转换到故障安全状态。

CONTROLSAFE 紧凑型车载平台构架

雅特生科技的 ControlSafe 紧凑型车载平台是由两台冗余 C-CCC 组成的系统，每台 C-CCC 都具备故障安全功能，联合实现高度可靠的平台。两台 C-CCC 之间则借助线缆直连方式 (DCA) 连接。DCA 负责实时监控平台内部两台 C-CCC 的运行健康状态。在初始状态下，DCA 会指定其中一台 C-CCC 为“主机”，另一台 C-CCC 为“备机”。在“主机”C-CCC 上运行的用户应用程序可以完全控制所有的输入/输出。在“备机”C-CCC 上运行的同一用户应用程序虽亦可监控安全相关的输入，但在默认情况下无法驱动任何安全相关的输出。作为“主机”的 C-CCC 发生失效时，其安全相关输出会受到抑制，并会通过 DCA 发出相应的状态信号，DCA 随即将“备机”C-CCC 切换为“主机”，并开始驱动安全相关的输出。而出现故障的 C-CCC 则被隔离到系统外不再参与运行，直至由维修人员重新修复。监控两台 C-CCC 的运行健康状态并控制两台 C-CCC 间的故障转移操作，从而实现高度可靠的故障安全计算系统。



主机 / 备机控制

雅特生科技的 ControlSafe 紧凑型车载平台支持采用线缆直连方式实现主机/备机切换控制。

线缆直连 (DCA)

线缆直连方式利用雅特生科技的专利算法和专用电缆连接两台 C-CCC。为了控制“主机”和“备机”之间的角色切换，系统需要通过运行在 CPU 模块上的特殊组件对两台 C-CCC 的健康状态信息进行实时的交换和跟踪。当系统上电时，首台接收到信号表明两片 CPU 模块均处于健康状态的 C-CCC 将成为“主机”。线缆直连方式 (DCA) 的设计意图也在于保证每次仅有一台 C-CCC 可以成为“主机”，而且只有健康的 C-CCC 才能成为“主机”。

安全继电器盒（SRB）

对于偏好或需要安全继电器的客户，可选择安全继电器盒 (SRB) 作为替代方式来连接 ControlSafe 紧凑型车载平台的两台冗余 C-CCC。在此情况下，SRB 的运行方式与 ControlSafe 安全平台相同（ControlSafe 安全平台是雅特生科技 ControlSafe 产品组合中的首款 SIL4 认证安全平台）。当作为“主机”的 C-CCC 发生失效时，SRB 会通过继电器和离散逻辑选择主机 C-CCC，并将控制权转交给先前作为“备机”的 C-CCC。SRB 还保证在任何时刻，至多仅能有一台 C-CCC 可以“主机”的角色运行，而且处于“非健康”状态的 C-CCC 是不能被切换为“主机”的。但是，初始版 ControlSafe 车载平台的 SIL4 认证仅涵盖基于线缆直连的配置。如果客户需要在 SIL4 应用环境中部署基于 SRB 的 C-CCC 解决方案，请联系雅特生科技的区域销售团队对此进行进一步讨论。

输入 / 输出模块开发

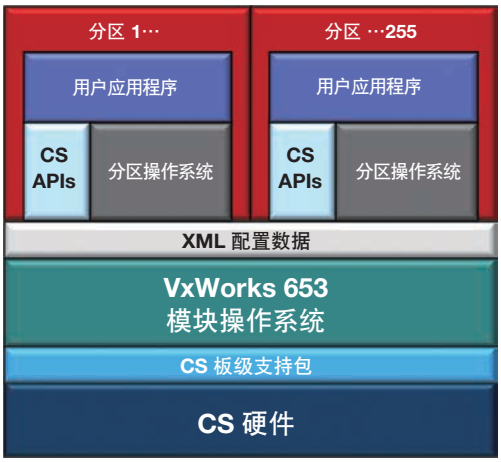
ControlSafe 紧凑型车载平台设计为通用基础平台，可通过连续追加雅特生科技 IOU 模块的方式实现各种应用。此外，雅特生科技还有助于客户灵活开发 IOU 模块和指定输入/输出背板连接，以通过提供所有必要的技术规格、产品支持和服务来满足客户的特定需求。此商业模式旨在增强雅特生科技与客户之间的合作，帮助客户有效且高效地利用可用资源来处理具有不同要求级别的项目。

可选集成风扇冷却子系统

为了使客户能够应对各种操作环境，雅特生科技还提供有可选集成风扇冷却子系统，以确保装满电源单元且完全运转的 ControlSafe 紧凑型车载平台机箱能够在 -40 ℃ 至 +70 ℃ 的进气口环境温度下正常运行。主动式空气冷却子系统由一个固定在机箱底部的安装盘位和一个 1U 可热插拔模块化自主风扇托盘（仅在进气口环境温度超过最低温度阈值时启动）组成。即使出现单个风扇故障，风扇托盘也可实现充分冷却。冷却系统在运行时，气流方向为由下而上。风扇托盘配有控制器，其运行状态由前面板 LED 指示，并且 ControlSafe 紧凑型车载平台可通过 I²C 接口对其进行轮询。

操作系统

ControlSafe 紧凑型车载平台支持面向用户可编程模块的风河 VxWorks 653 操作系统和编程环境，特别是 CPU、SWM 和 CAN。VxWorks 653 不仅提供资源管理，而且还提供分区环境，从而允许不同安全级别的多个独立应用程序可运行在处于保护状态下的同一目标平台上。VxWorks 653 的核心组件是 Core OS。Core OS 组件利用目标架构的特性，能够加强对独立分区内运行的应用程序之间的安全隔离。这些分区可安装由以下三个接口层中任意一个所支持的应用程序软件：基于 VxWorks 的 API、APEX 接口（ARINC 653 接口）或 POSIX API。这些接口层为应用程序提供多层级的调度和线程管理。另外，除了分配分区内存和 CPU 时间占用，Core OS 还提供各类管理系统资源服务，例如输入 / 输出。



CS - ControlSafe

Core OS 通过静态定义的配置表执行分区定时任务。该配置表不仅可为每个分区分配 CPU 周期，并且还可指定分区的执行顺序。Core OS 为各应用程序分区来统一管理所有的共享资源，其中包括系统时间和内存。此外，Core OS 能确保在分区切换后，应用程序分区能分配到所需的资源，而且能防止应用程序间的互相损坏。只有当使用了合适的信道并被系统配置表允许时，分区之间以及分区与 Core OS 之间的通信才能进行。

VxWorks 653 健康监控（HM）提供发起和处理事件的框架，比如说，该事件可以是综合模块化航电（IMA）系统中的报警或消息。此框架支持 ARINC API，而且包括一个独立的 API。HM 在三个层级发挥功能：模块、分区和进程。错误响应和恢复执行在分区和模块层级由表格驱控，而应用程序执行则是在进程层级进行驱控。分区或模块层级处理程序可通过向其它分区通知既定事件的方式将信息传递给其它分区。例如，一个分区处理程序可以告知其它分区导致了该分区重新启动的事件。

应用程序编程接口 (API)

为了帮助客户提高安全应用程序的开发效率，雅特生科技将向客户提供了详尽的应用程序编程接口（API）。借助 API，客户可方便快捷的调用程序来执行各种任务，例如，查询安全逻辑的状态、协助各层级间的通信，以及监控系统内存等关键组件的健康状况。除此之外，雅特生科技还提供一系列控制和状态 API 以使安全应用程序具备更为细致的系统控制能力，例如，对 watchdog 定时器和输入 / 输出端口的控制，以及对设备硬件物理健康的监控。供为参考，以下是 API 的主要类型列表：

- 控制 / 状态
- DRAM 数据清理程序
- 固件升级
- 闪存完整性
- 链路健康检查
- 日志记录
- 维护模式监视器
- 网络路由
- 永久性 DRAM
- 平台管理
- 运行时间诊断
- 切换管理
- 安全层
- 重要产品数据 (VPD)
- 表决逻辑

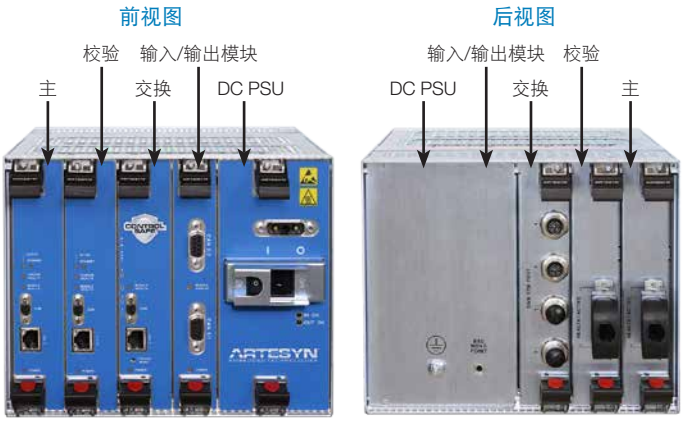
认证文档

雅特生科技的 ControlSafe 车载平台严格遵循所有适用的业界规格和标准，为现代安全应用程序提供高可靠和高可用性平台。雅特生科技将向客户提供完整的安全认证文档，以协助其顺利通过最终集成系统的安全认证。

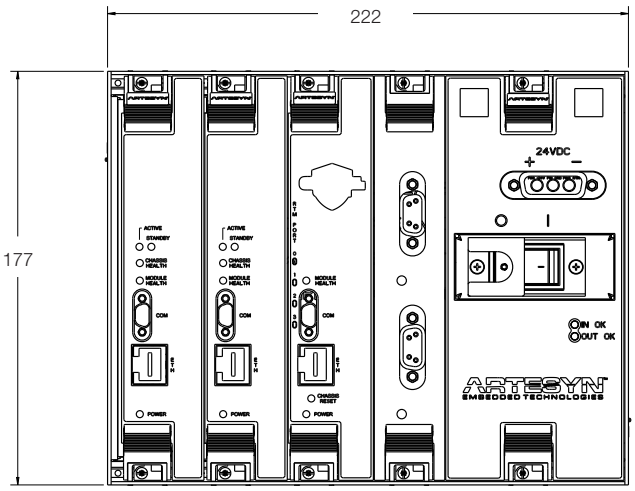
这些安全认证文档包括：

- 安全案例
  - 系统定义
  - 质量管理报告
  - 安全管理报告
  - 技术安全报告
- 安全评估报告
- 安全手册
  - 规定相应的用户动作，以确保其能够将雅特生科技的 ControlSafe 紧凑型车载平台顺利集成到安全相关系统中去
- 由认证机构签发的安全认证证书

系统机箱

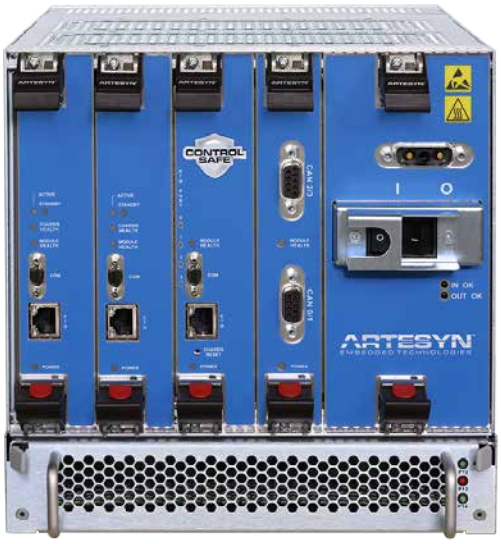


CONTROLSAFE 紧凑型车载计算机尺寸

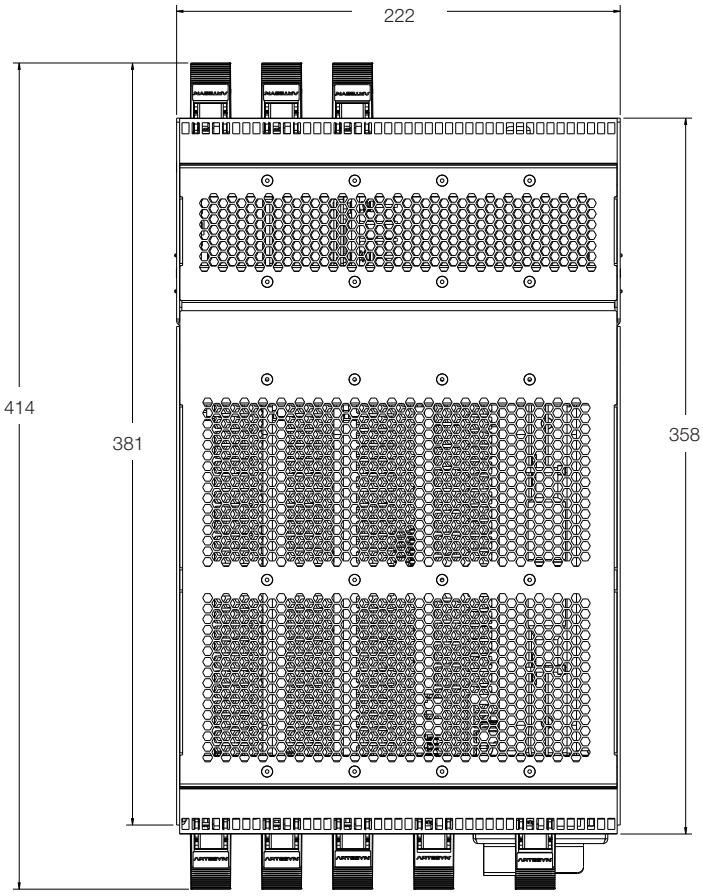


可选集成风扇冷却子系统

风扇托盘



带有风扇托盘安装盘位的 C-CCC 机箱



单位：mm

技术规格

	CPU 模块	*交换模块和 CAN IOU 模块*	*UART 和数字 IOU 模块*
处理器	NXP P2020 (1 GHz)	NXP P10110 (800 MHz)	Altera Cyclone V SoC 和 FPGA
操作系统	风河 VxWorks 653	风河 VxWorks 653	Linux（用户不可编程）
内存	1GB（可选 4GB）DDR3-800 SDRAM, ECC	512MB（可选 2GB）DDR3-667 SDRAM, ECC	512MB DDR3-800 SDRAM, ECC
闪存	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
维护端口	10/100/1000 BASE-T 和 RS-232	10/100/1000 BASE-T 和 RS-232（仅限交换模块）	RS-232
数据交换	四 (4) 路 GbE 链接		
单板管理	电压和温度传感器		

输入 / 输出端口	
IOU 插槽数量	一 (1) 个
10/100/1000 BASE-T 以太网端口	标配：交换模块配四 (4) 个端口
控制器局域网总线端口	选配：每个 CAN IOU 四 (4) 个端口
串行 UART	选配：每个 UART IOU 配八 (8) 个端口
数字输入	选配：每个数字输入 IOU 配十六 (16) 个端口
数字输出	选配：每个数字输出 IOU 配八 (8) 个端口

物理规格		
运行温度	-40 ℃ 至 50 ℃	开放式机架环境中
	-40 ℃ 至 70 ℃	具有所需气流（于机箱底部的进气口处测得）的封闭机架装置内；或采用可选集成风扇冷却解决方案
冷却	强制通风和对流冷却	
电源	直流：24V (16.8 - 30 VDC)	
振动	符合 EN 61373，种类 1，B 类 (EN 50155 12.2.11) 标准	
震动	符合 EN 61373，种类 1，B 类 (IEC 60068-2-27) 标准	
机箱密封	标配：IP20；选配：IP30	
保形涂层	EN50155 第 12.2.10 节（盐雾试验）ST1 级别	
规范标准	遵循下列标准设计：EN50121、EN50124、EN50155、EN50126、EN50128、EN50129、EN55024、EN60529、EN60571、IEC61508。欲了解更多信息，请参阅相关文档。	
安全认证	EN50126、EN 50128、EN50129 (SIL4) 和 IEC61508 (SIL3)	

订购信息

组件号	*描述*
CSP-C-CCC-CORE-DC-01	4U ControlSafe 紧凑型车载计算机核心，包括一个机箱、一个直流电源装置、两个 CPU 模块和一个交换模块
CSP-C-CCC-CORE-DC-02	4U ControlSafe 紧凑型车载计算机核心，包括一个机箱、一个直流电源装置、两个 CPU 模块、一个交换模块和一个 1U 经济型风扇冷却系统
CSP-C-CCC-CORE-DC-03	4U ControlSafe 紧凑型车载计算机核心，包括一个机箱、一个直流电源装置、两个 CPU 模块、一个交换模块和一个 1U 高级风扇冷却系统
CSP-CCC-CAN-01	4 端口 CAN 输入/输出模块
CSP-C-CCC-UART-01	8 端口 UART 输入/输出模块
CSP-C-CCC-DI-01	16 通道数字输入模块
CSP-C-CCC-DO-01	8 通道（双切）数字输出模块
CSP-C-CCC-CHAS-FAN-02	经济型替换风扇托盘 FRU
CSP-C-CCC-CHAS-FAN-03	高级替换风扇托盘 FRU
CSP-C-CCC-FAN-BAY-01	1U 盘位安装套件，用于风扇托盘 FRU
CSP-C-CCC-FILL-01	5HP 填充面板
CSP-C-CCC-BAY-FILL-01	填充面板，用于盘位安装套件
CSP-CSC-SRB-01	安全继电器盒（SRB）
CSP-CSC-SRB-FRU-01	安全继电器盒的可更换模块
CSP-CBL-DIRECT-01	两条电缆（用于线缆直连 (DCA) 运行）
SERIAL-MINI-D2	串行电缆 —— 微型 D-sub 连接器，符合 DE9 标准

解决方案服务

雅特生科技可提供一整套经过优化的解决方案服务，从而可在整个产品生命周期中满足您的要求。设计服务有助于缩短上市时间。部署服务包括全球范围 24 小时全天候技术支持。更新服务可确保产品寿命更长和技术更新。

全球办事处

美国	+1 888 412 7832	日本	+81 3 5403 2730
香港	+852 2176 3540	韩国	+82 2 6004 3268
中国	+86 400 8888 183		

ARTESYN™
EMBEDDED TECHNOLOGIES

www.artesyn.com