COMPUTING

# ControlSafe™ プラットフォーム(CSP)

## 列車制御と鉄道信号向けSIL4 COTS フェイルセーフシステム

### データシート

- SIL4安全度規準に認証される様にデザインされた、高度に統合されたCOTSプラットフォーム
- シックス・ナイン(99.9999%)のシステム可用性を提供する為のデザイン
- 鉄道用途向け多様なモジュールそして拡張性
- 革新的なデータ・ロックステップ・アーキテクチャにより、シームレスなアップグレード
- ハードウェアベースの多数決メカニズムが、アプリケーションソフトウェアを透明化
- 15年の製品寿命ベースに、25年の延長サポートそしてサービス
- グローバルなサービス体制によるサポート
- 将来の車両や鉄道開発のための製品ポートフォリオ

アーティセン・エンベデッドテクノロジーズは、30年以上にわたる高信頼性と高可用性のエンベデッド・コンピュータシステム開発の専門性を活かし商用市販品(COTS)フェイルセーフコンピュータシステムを、鉄道システムのインテグレータそして鉄道用アプリケーションプロバイダへ提供するトップサプライヤです。

全ての信頼性、可用性、保守性、安全性(RAMS)プロセスはEN50126、全ての安全関連のソフトウエアはEN50128、そしてハードウェアはEN50129に認証される様にデザインしたアーティセン のControlSafe™プラットフォーム(CSP)は、SIL4セーフティアプリケーション環境で展開できます。

オープンスタンダードに基づくアーティセン のControlSafe™ プラットフォーム（CSP）は、鉄道用アプリケーション開発者やシステムインテグレータにとって厳しいSIL4システム開発とその認証プロセスに伴う高いコストとリスクに阻まれず、タイム・トゥ・マーケット期間の大幅短縮を可能にできるコスト効率の良いソリューションです。

アーティセンは、一貫した信頼できるシステムを、顧客と長期パートナーシップを結びサポートします。このControlSafeプラットフォームは、15年の製品寿命をベースに、25年の延長サービスを、高信頼性プラットフォームで提供できることが鉄道顧客様への更なる強みになります。

アーティセンのControlSafeプラットフォームのデザインは、クラス最高の99.9999%という高いシステム可用性を提供する様デザインされた、これはシステムのダウンタイムが1年あたり数秒以下になることを意味します。アーティセンは高度技術を有するスタッフチームによる広範なモデル化と解析を成功裏に完了させ、鉄道規格とその仕様で定められたあらゆる機能安全性、信頼性、可用性要件に適合することを確認しています。

アーティセンの将来性を考えたこのControlSafeプラットフォームは、モジュラー、スケーラブル、そして製品ライフサイクルと通し必要となる追加のI/Oインターフェースやプロセッサのアップグレードをシームレスにできるよう設計されています。

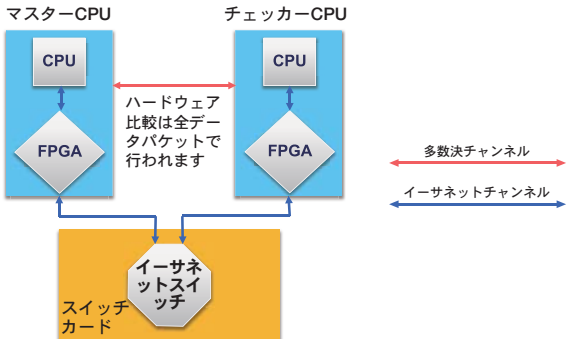
包括的な製品ラインを確立するため、アーティセンはプラットフォームの継続的な開発に注力しています。第一歩となるのはディスクリート拡張I/Oボックスの開発で、顧客はこれにより当社のControlSafe プラットフォームを各種の鉄道信号用アプリケーションにシームレスに統合することが可能になります。当社の最終的な目標は、顧客側がエンドアプリケーション差別化に開発努力を注力できることで、顧客の競争力を強化することにあります。

アーティセンのControlSafe™ プラットフォーム(CSP)

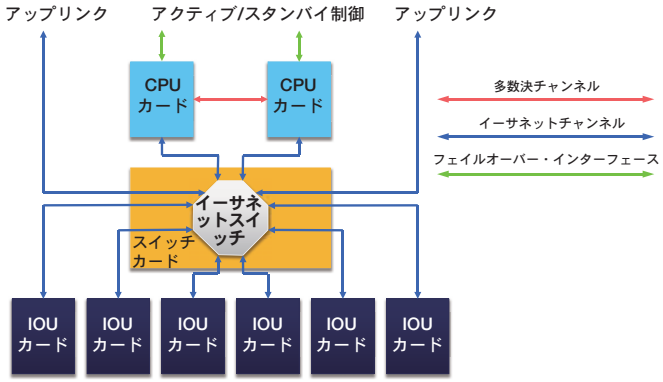
ARTESYN™
EMBEDDED TECHNOLOGIES

## ControlSafe™コンピュータアーキテクチャ

各ControlSafe™コンピュータ(CSC)の中枢にある２基の同一のCPUボードで、データ・ロックステップモードを動作し、2 out of 2(2oo2)の多数決メカニズムが実行されます。データロックステップモードでは、２基のCPUのデータファブリック・インターフェースに判定境界を設けます。この判定境界を経由するあらゆるトランザクションは、２基のCPUの正確な動作を確認するために比較されます。プロセッサのクロック周波数が同期し、判定境界がアドレスとプロセッサのデータバスで生成されるハード・ロックステップモードとは異なり、データ・ロックステップモードは、最新の高性能プロセッサを使用して実行することだができます。



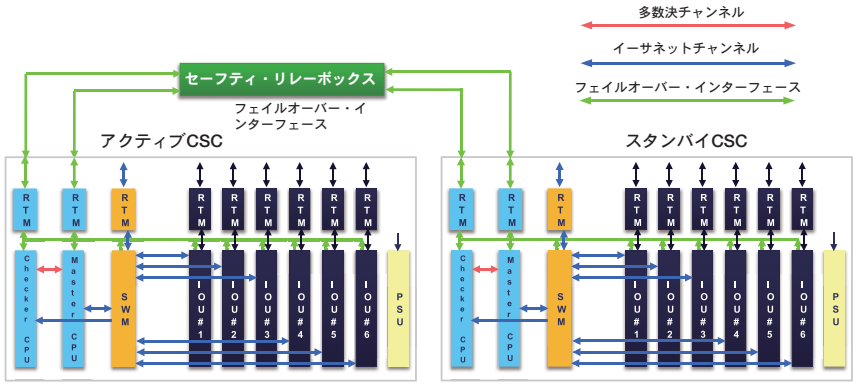

データファブリックのバウンドトランザクションの比較は、2oo2多数決メカニズムにより行われ、２基のCPUに相違があると障害と判断され、CSCはフェイルセーフモードに入ります。フェイルセーフモードでは、全ての出力ポートはデフォルトでセーフ状態に入り、外部機器が誤った状態に設定される可能性を排除します。




このControlSafe™ プラットフォームのデータ・ロックステップアーキテクチャにより、同一のI/Oを使いながらプロセッサをアップグレードすることが可能です。2 out of 2(2oo2)多数決機能がハードウェアに搭載されているため、アプリケーション開発者は、既存のアプリケーションソフトウェアを最小限の変更でマイグレーションすることが可能になります。

I/Oモジュールは、CAN、イーサネット、イーサネットリング、UART、MVBなど様々な範囲の通信プロトコルへのインターフェースを提供します。全I/Oモジュールは、同一のフリースケールCPUコアとウインドリバーVxWorks 653オペレーティングシステムに基づいた、共通のアーキテクチャを持っており、ソフトウェア開発環境を簡素化します。全I/Oモジュールは、イーサネットを介してアクセスされ、シームレスな分散型アーキテクチャを可能にします。全モジュールは、システム動作不能リスクのない形でソフトウエアとファームウエアのリモートでのオンラインアップグレードが可能です。全てのI/Oポートは、セーフティと非セーフティとしてユーザプログラマブルです。さらにスイッチモジュールは、アプリケーション・ネットワーク内の他の処理ノードへのダイレクトイーサネット/IPアクセスのために、リアトランジションモジュールを介した８基の10/100/1000BASE-Tポートを備えています。

## ControlSafe™プラットフォームアーキテクチャ




このControlSafeプラットフォームは、 2 台の冗長化ControlSafe コンピュータ(CSC)で構成され、それぞれにフェイルセーフ動作が備わっています。それらは、 2 台のCSCの正常性を監視し、 1 台を「アクティブ」、他方を「スタンバイ」に指定しするセーフティ・リレーボックス(SRB)、又はダイレクトコネクト・アルゴリズム(DCA)にリンクされています。アクティブなCSC上で動作するユーザー側アプリケーションは、全I/Oポートへのフル制御を有し、一方スタンバイCSC上で動作する同じユーザー側アプリケーションは、セーフティ関連の入力ポート（イーサネットI/Oモジュールを除く）と、全てのポートを監視可能です。しかしデフォルトに於いて出力ポートの制御はできません。　アクティブなCSCは障害があるとセーフティ関連の出力ポートは休止され、SRBにその状態を信号で伝え、SRBはスタンバイCSCをアクティブにしてその出力を作動させます。その故障したCSCは、オペレーションから外されます。一旦それがサービス要員によって修理されれば、またサービスの中に戻す事ができます。CSC 2 基の正常性監視と 2 基間のフェイルオーバー動作を制御することで、フェイルセーフな、コンピュ―ティングシステムを実現しています。

## アクティブ/スタンバイ制御

アーティセンのControlSafe プラットフォームは、2モードのアクティブ/スタンバイ制御をサポート：セーフティ・リレーボックスオプションとダイレクトコネクトオプション。

## セーフティ・リレーボックス

SRBはアクティブなCSCを選択し、そのアクティブCSCに障害があるとスタンバイCSCに制御を移します。SRBは 2 基の冗長性セーフティリレーフィールドリプレイサブルユニット(FRU)、ケーブル、パワーフィードで構成され、継続的な可用性が保証されています。各CSC は、2基のセーフティリレーFRUの 1 つに接続されています。

SRBは電力が供給されると、両CPUが正常である旨の信号を送った最初のCSCをアクティブCSCとして選択します。他方のCSCは、スタンバイモードになります。アクティブCSCは障害を検出するとSRBにその異常状態を信号で伝えます。スタンバイCSCが正常な場合は、SRBが信号を送りそれをアクティブにします。SRBは、一度に 1 基のCSCだけがアクティブになることができ、異常のあるCSCがアクティブになれないように設計されています。

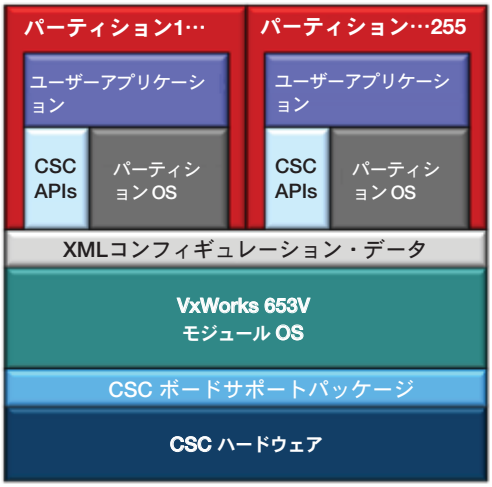
アーティセンのSRBは、オンラインサービスとセーフティリレーFRUレベルの修復をサポートし、ControlSafe プラットフォームの動作時間を最大限にしています。サービスモードはセーフティリレーFRUの手動の 2 ポジションスイッチで選択でき、スイッチを「オート」から「サービス」に切り替えると、接続されたCSCがスタンバイモードになります。

## ダイレクトコネクト

ダイレクトコネクトオプションは、特許のアルゴリズムとCSC 2 基を繋ぐ専用ケーブルを使用します。全CPUモジュール上で動作するステートマシンで正常性ステータスを交換、トラッキング、アクティブとスタンバイの役割を制御します。電力が供給されると、両CPUからの信号が正常な最初のCSCがアクティブになります。SRBの場合と同様に、ダイレクトコネクト・アルゴリズム（DCA）は、一度に 1 基のCSCだけがアクティブになることができ、正常なCSCだけがアクティブになることを保証します。

## オペレーティングシステム

ControlSafe プラットフォームの全モジュールはウインドリバーVxWorks 653オペレーティングシステムをサポートしています。そのためリソース管理及び、重要度レベルが異なる複数アプリケーションを、単一ターゲットプラットフォーム上で保護状態で動作可能なパーティショニング環境の双方を提供しています。VxWorks 653の中核はコアOSです。このコアOSコンポーネントはターゲットアーキテクチャの特長を利用し、別パーティションに分けられたアプリケーション間の独立性を強化します。これらのパーティションには、 3 つのインターフェースレイヤ：VxWorksベース API、 APEX インターフェース (ARINC 653インターフェース)、POSIX API の 1 つにサポートされたアプリケーション・ソフトウェアを入れることができます。これらインターフェースレイヤは、アプリケーションに対する異なるレベルのスケジューリングとスレッドを提供します。コアOSは、パーティションメモリとCPU使用率の管理だけでなく、I/Oなどのシステムリソース管理機能もあります。




コアOSは、各パーティションへのCPUサイクル割当てとパーティションの実行順序を設定する静的に定義された構成表を使用し、パーティションスケジューラを実行します。コアOSはアプリケーションパーティションのために、システム時間・メモリを含む全共有リソースを制御します。コアOSはパーティション切り替え後に、アプリケーションパーティションが必要とするリソースを確保し、アプリケーション相互の破損を防止します。パーティション相互間、またパーティションとコアOS間の通信は、適切な通信チャンネルが使用された場合、及びシステム構成表でそのチャンネルが許可された時のみ実行されます。

VxWorks 653のヘルスモニタ (HM)は、統合化アビオニクス(IMA)システムのアラームやメッセージ等のイベントの発信、管理を行うフレームワークを提供します。このフレームワークは、スタンドアロンAPI を含むARINC APIをサポートしています。HMは、モジュール、パーティション、プロセスの 3 レベルで機能します。フォールト応答と復旧動作はパーティション及びモジュールレベルでのテーブル駆動で、アプリケーション駆動はプロセスレベルです。パーティション又はモジュールレベルのハンドラは、発生したイベント通知を他のパーティションに通信可能です。例えば、あるパーティションハンドラは、他のパーティションに再起動の要因となるイベントを通知することができます。

## アプリケーション開発環境

VxWorks 653プラットフォームには、エンドツーエンドのソフトウェア開発スイートを提供するEclipseベースのツールコレクション、ウインドリバー Workbenchが含まれています。Workbenchは、ホスト・ターゲット間通信の確立/管理、VxWorks 653モジュールの開発、動作、デバッグ、モニタ、解析、テスト、制御をサポートしています。Workbenchには、総合的な開発プロジェクト機能、先進のソースコード解析、複数ターゲットの同時制御、単一又は複数ターゲットのマルチプロセスやマルチスレッドを管理するデバッガが含まれています。またWorkbenchには、コンフィギュレーションツール及びビルドツールが含まれ、XMLとコンポーネントベースを組み合わせたコンフィギュレーション、VxWorks 653モジュールのビルドをサポートしています。さらにグラフィカルインターフェースを使用しない開発者のために、プロジェクトのビルド、XMLとコンポーネントによるコンフィギュレーション、ランニングシステムのモニタとデバッグを行う認証済みコマンドラインツールを提供しています。

そして特別なハードウェアの必要性無しにWindowsプラットフォーム上で、VxWorks 653アプリケーション作成しテストする能力を可能にするVxWorks 653シミュレータも含まれています。VxWorks 653環境は、WTX（ウインドリバー・ツ―ルエクスチェンジ）プロトコルをサポートし、そのためホストアプリケーションとホストコンピュータのターゲットサーバ間の通信を可能にしています。WTXはまた、サードパーティアプリケーションのWorkbench GUIへの接続にも使用できます。

## アプリケーションプログラミングインターフェース

アプリケーションプログラミングインターフェース(API)のライブラリが、セーフティアプリケーションのビルドプロセスを容易にするために提供されます。これらはセーフティロジックの状態の問い合わせ、レイヤ間の通信を補助、そしてシステムメモリの様な重要なコンポーネントの状態をモニタする機能を提供します。さらに、セーフティアプリケーションにウォッチドッグタイマレベルの管理、I/Oポート制御、物理的正常性モニタのフル制御を可能にする一連のコントロールとステータスAPIがあります。以下がそのAPIのリストです。

- コントロール/ステータス
- DRAM スクラバ
- ファームウェアヘッダ情報
- ファームウェア・アップグレード
- IPアドレス
- リンクヘルスチェック
- モジュール管理
- PRP/HSRスイッチング管理
- ランタイム診断
- セーフティレイヤ
- システムロギング
- スイッチング管理
- 重要プロダクトデータ(VPD)
- 多数決論理

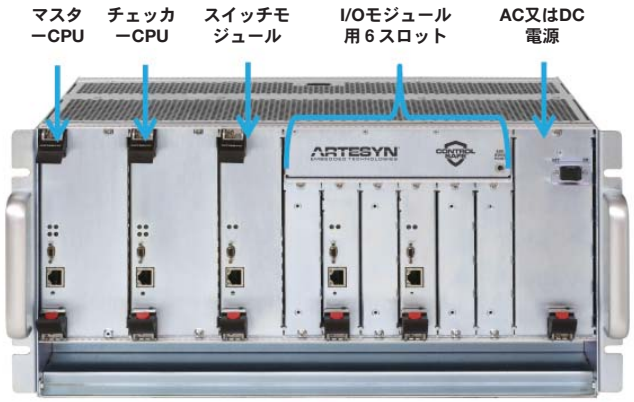
## SIL4認証エビデンス

アーティセンのControlSafe プラットフォームは、モダン・セーフティアプリケーション用の高度な信頼性と可用性あるプラットフォームに要求される、あらゆる業界仕様と規格に厳格に従っています。アーティセンのControlSafe プラットフォームは、顧客に完全な認証エビデンスパッケージを提供し、その統合システムに対する認証プロセスを円滑化します。認証エビデンスパッケージには次のものが含まれます：

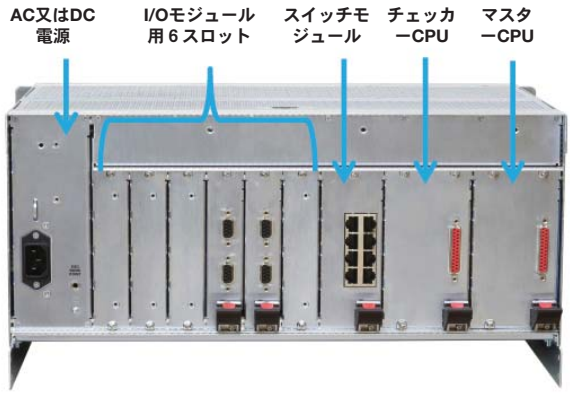
- セーフティケース
  - システムの定義
  - 品質管理レポート
  - 安全管理レポート
  - 技術的安全性に関わるレポート
  - 安全性評価レポート
- セーフティマニュアル
  - 安全関連システムへのアーティセンの ControlSafe プラットフォームの統合を可能にするために必要なユーザーアクションの特定
- 認証機関が発行したSIL4認証

## システムシャーシ

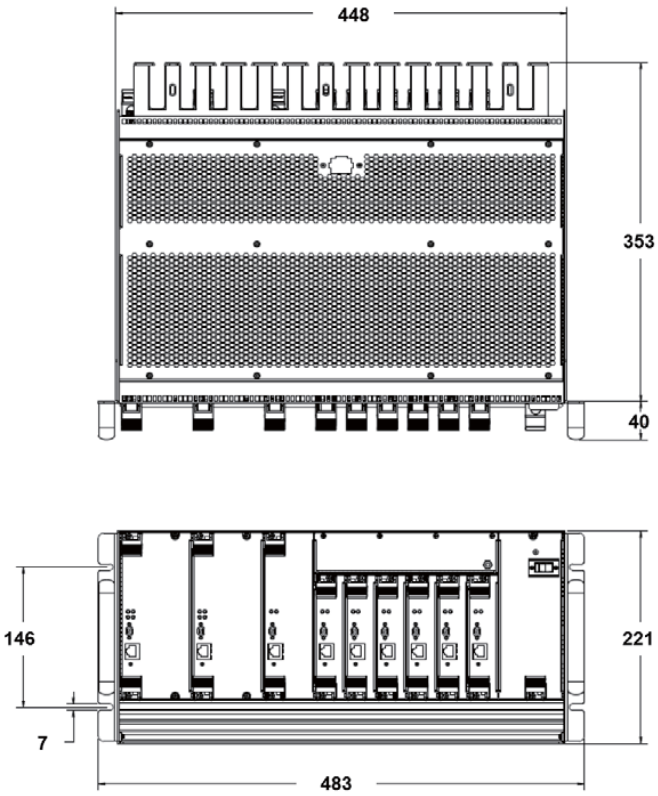
### 前面図



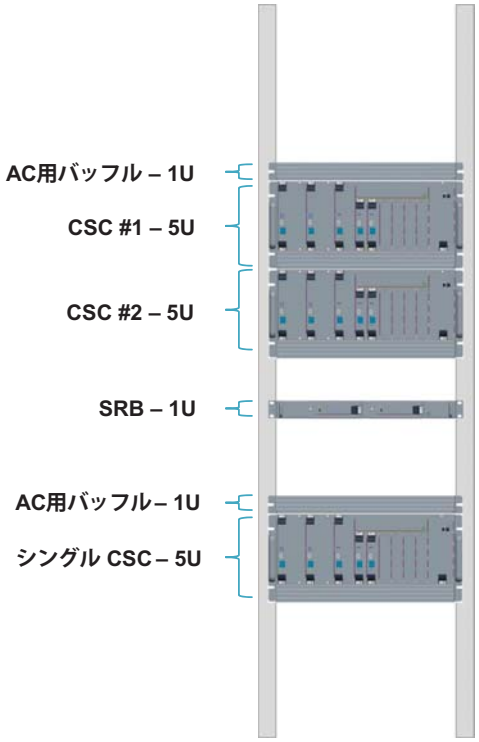

### 後面図




### CSC寸法（単位：mm）




### システムラックマウント例



## 技術仕様

| | *プロセッサモジュール* | *スイッチモジュール及びIOUモジュールプロセッサ* |
|---|---|---|
| プロセッサ | フリースケールP2010 (1GHz) | フリースケール P1011 (800MHz) |
| オペレーティングシステム | VxWorks 653 | VxWorks 653 |
| メモリ | 1GB (オプションで 4GB) DDR3-800 SDRAM, ECC | 512MB (オプションで 2GB) DDR3-667 SDRAM, ECC |
| フラッシュ | 2 X 128MB NOR | 2 X 64MB NOR |
| MRAM | 2 X 2MB MRAM | 1 X 2MB MRAM |
| メンテナンスポート | 10/100/1000 BASE-T 及び RS232 | 10/100/1000 BASE-T 及び RS232<br>(スイッチモジュール用のみ) |
| データファブリック | 1GigE | |
| ボード管理 | スロット、電圧、温度センサ | |

| | *I/Oインターフェース* |
|---|---|
| I/Oスロット数 | 6 |
| 10/100/1000 BASE-T イーサネット | イーサネットIOUにつき標準：8；オプション：2 |
| イーサネットリング | オプション：イーサネットリングIOUにつき2 |
| CANbus | オプション：CAN IOUにつき2 |

| | *物理的仕様* |
|---|---|
| 動作温度 | -40 ℃ から +70 ℃ |
| 冷却 | 対流冷却 |
| 電力 | DC: 100VDC 公称 (66~127.5V) AC: 90~264V, 47~63Hz |
| 振動 | EN61373 (12.2.11)準拠 |
| 衝撃 | IEC 60068-2-27準拠 |
| シャーシシーリング | 標準：IP20；オプション： IP30 |
| 絶縁保護コーティング | ST1等級、EN 50155セクション 12.2.10 (塩水噴霧試験) |
| 標準準拠 | EN50121、EN50124、EN50155、EN50126、EN50128、EN50129、EN55024、<br>EN60529、EN60571、IEC61508準拠設計。個別の準拠性については文書をご覧下さい。 |

## 製品のご注文

| *部品番号* | *説明* |
|---|---|
| CSP-CSC-CORE-AC-01 | シャーシx1、AC PSUx1、CPUモジュールx2、スイッチモジュールx1で構成 |
| CSP-CSC-SRB-01 | セーフティ・リレーボックス |
| CSP-CSC-SRB-FRU-01 | セーフティ・リレーボックス用交換ユニット |
| CSP-CSC-CAN-01 | CAN I/Oモジュール |
| CSP-CSC-CAN-RTM-01 | ハイスピード・リアトランジションモジュール、CAN I/Oモジュール用 |
| CSP-CSC-RING-01 | イーサネットリング・モジュール |
| CSP-CSC-RING-RTM-01 | リアトランジションモジュール、イーサネットリング・モジュール用 |
| CSP-CSC-ETH-01 | イーサネットI/Oモジュール |
| CSP-CSC-ETH-RTM-01 | イーサネットI/Oモジュール用リアトランジション・モジュール |
| CSP-CBL-MATN-01 | メンテナンス用ケーブルキット |
| CSP-CBL-PWR-B-01 | 電源コード、米国/カナダ/日本用 |
| CSP-CBL-PWR-EU-01 | 電源コード、韓国/ドイツ/イタリア/フランス用 |
| CSP-CBL-PWR-I-01 | 電源コード、中国用 |
| CSP-CBL-SRB-01 | ControlSafeコンピュータのセーフティ・リレーボックス接続用ケーブルx2 |
| CSP-CBL-DIRECT-01 | ControlSafeコンピュータ2基直接接続用ケーブルx2 |
| CSP-CSC-FILL-01 | フロント・フィラーパネル |
| CSP-CSC-FILL-RTM-01 | リア・フィラーパネル |

## SOLUTION SERVICES

Artesyn Embedded Technologies 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 global 24x7 technical support. Renewal services enable product longevity and technology refresh.



## WORLDWIDE OFFICES

**Tempe, AZ U.S.A.** +1 888 412 7832
**Shanghai, China** +86 21 3395 0289
**Munich, Germany** +49 89 9608 2552
**Tokyo, Japan** +81 3 5403 2730
**Hong Kong** +852 2176 3540
**Seoul, Korea** +82 2 3483 1500



ARTESYN™
EMBEDDED TECHNOLOGIES

www.artesyn.com