



組み込みセキュリティに光を IoTへの対応

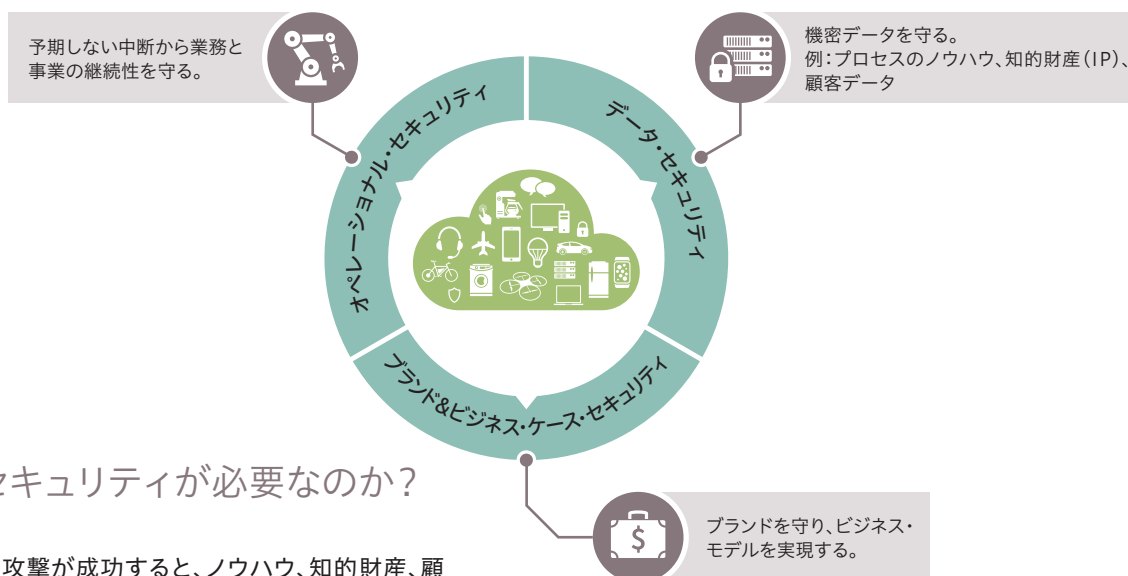
www.infineon.com/embedded-security



組込みセキュリティへの不安の高まり

組込みシステムはどこにでもあるものになりつつあります。モノのインターネット(IoT)やマシン・ツー・マシン(M2M)通信の普及は、ネットワーク化されたデバイスや装置の増加を意味します。小さな家電から、大規模通信ネットワークや複雑な産業オートメーション・システムまで、多くが専用の組込みコンピューティング・システムによって制御されています。

ネットワーク化の流れは速度を増し続け、ユーザには一層の便利さと快適さを、企業には新しいビジネスやサービスのモデルをもたらします。しかし、組込み分野のセキュリティは、大きく遅れがちです。攻撃対象が広がるにつれて、セキュリティ上の脆弱性が飛躍的に高まり、秘密データや知的財産(IP)、工程の整合性を守ることにメーカーは苦戦しています。



なぜ組込みセキュリティが必要なのか？

組込みシステムへの攻撃が成功すると、ノウハウ、知的財産、顧客データ、プロセス・インテリジェンスといった機密情報が漏れる恐れがあります。また、攻撃によって業務が中断すれば、事業の継続性を損ない、企業のブランド・イメージや業績、存続そのものを危険にさらします。

課題

- › より巧妙で強力になってゆくハッカーの攻撃からシステムを守る。
- › 守りたい資産の価値と予算の制約とをバランスさせる。
- › 確実で信頼できる、実装可能なセキュリティ機能を見つける。
- › 使いやすさを犠牲にせずに、システムのセキュリティを向上させる。

目的

- › 新しいビジネスやサービスのモデルを開発する。
- › イメージしやすく競争力のある差別化を考える。
- › パートナーのノウハウを活用することで、セキュリティへの投資を削減する。
- › サプライチェーン全体の管理を改善し、生産工場の選択の幅を高める。



提案

組込みセキュリティの課題に見合った、実装が簡単で、スケーラブルかつカスタマイズが可能なソリューション OPTIGA™ があります。

信頼できるアドバイザーとして、インフィニオンが複雑さや実装コストの削減を、お手伝いします。セキュリティのノウハウやインフラストラクチャへ投資するよりも、ハードウェア方式のセキュリティ・ソリューションについて豊富な実績を持つインフィニオンの専門知識をご活用下さい。



脅威への防御

ソフトウェアは比較的簡単に読み出して、複製や配布ができるため、それだけでは組み込みシステムを守るのに不十分です。データとプログラムを確実に保管し、外部からの不正操作を検出し、安全な保管や処理のためにデータを暗号化するには、セキュアなハードウェアが必要です。信頼の基点「ルート・オブ・トラスト」を設けて組み込みソフトウェアを信頼できるものにするために、ハードウェア方式を採用したインフィニオンのソリューションをご活用下さい。

OPTIGA™ は、セキュリティ上重要な三つの基本機能をサポートして、ルート・オブ・トラストを実現します。

› 認証

OPTIGA™ セキュリティICは、許可された人や機器の間でのみ情報が交換されるように、人や機器の認証を行います。

› 暗号化

セキュリティ・モジュールが暗号化や、秘密鍵の安全な保管を行い、秘密情報を守ります。

› 完全性

セキュリティ・チップがプラットフォームや装置、機器の完全性をチェックし、改ざんの特定と不正変更の検出を行います。

セキュリティ・アーキテクチャー上にルート・オブ・トラストを設けるハードウェア方式のソリューションは、IoTの可能性を最大限に活かせる安心感を全ての人に加え、消費者や企業へ莫大な恩恵をもたらします。

製品のセキュリティを越えて

セキュリティ分野で30年の実績を持つインフィニオンの取組みは、明確かつ確実なセキュリティ製品で、お客様を支援することだけではなくありません。

インフィニオンは、製品のセキュリティ面以外の数々の点でも、信用を得ています。第一は、工程のセキュリティを重視していることです。セキュリティ認定を取得した設計施設、生体アクセスを使った専用の設備、そして何よりも、鍵のプログラミングを保護するセキュアな生産体制を整えています。

第二には、セキュリティ・エキスパートが、最新製品を厳しくテストしています。新しい攻撃手法を追い、継続的に製品コンセプトへ反映させ、製品のライフサイクルを適切に保っています。

さらには、開発や製造の工程同様に、第三者認定を受けた製品を持っているということです。多くのインフィニオン製品が、ドイツ当局による厳格なコモン・クライテリア認定に合格しています。

これらの取組みは、インフィニオンのお客様が、その先のお客様の信頼を得るための明快な説明材料になります。

マーケットの広がり

セキュリティはニーズが複雑になるほど多様化します。基礎的な単純機能である認証ソリューションから、先進的なプラットフォームの完全性チェックのための堅牢な認定セキュリティ・モジュールまで、幅広い市場分野にわたる個々のセキュリティ・ニーズをサポートするために、業界最大の製品ラインアップを揃えました。

スマート・ホーム

エアコンのセンサーから家全体の制御システムまで、あらゆるものの保護を可能にします。

- › スマート・ホームのゲートウェイとサーバー間の通信をセキュアにする。
- › ホーム・オートメーション機器を認証する。
- › 偽のホーム・オートメーション機器から保護する。

実績のあるセキュリティ機能を使って、安心の新アプリケーションを立ち上げ、新しいビジネスやサービスのモデルを創出する全ての事業に柔軟性とコスト削減をもたらすことで、今日のスマート・ホームを魅力あるものにします。



コネクテッド・カー

ユーザの秘密データを守り、自動車をより安全にします。

- › テレマティクス・システムの通信をセキュアに行う。
- › インフォテインメント・システムを認証し、サービスを有効にする。
- › リモート・メンテナンスの情報やファームウェアのアップデートをセキュアに行う。

インフィニオンは、自動車分野での長年の経験とセキュリティの豊富なノウハウを活かした最適なセキュリティ・ソリューションで、コネクテッド・カーを実現します。新しいビジネスやサービスのモデルを見つけるチャンスです。



クラウド

情報・通信技術

スケーラブルな製品ラインアップが、小型ネットワーク・スイッチから大規模ネットワークまで、あらゆる通信とアクセスを保護します。

- ＞ ネットワーク機器間のセキュアな通信によりデータを保護する。
- ＞ ソフトウェアのアップデートをセキュアに行い、ソフトウェアを保護する。
- ＞ ルーターで管理されたネットワーク・アクセスによって機器の完全性をチェックする。

ICT分野での信頼されるパートナーとして、インフィニオンが幅広いパートナー・ネットワークを通じた実装やデバイス管理のサポートを提供し、最新セキュリティ・ソリューションを容易に導入頂くことで、お客様の優位性を保つことができます。信頼できるセキュリティ・ソリューションにより、新しいビジネスやサービスのモデルを創出できます。

スマート工場

装置のセンサーから制御システムまで、あらゆるものをセキュアにし、製造業の長期的な成功をお手伝いします。

- ＞ オートメーション・システムとITプラットフォーム間の通信をセキュアにし、秘密データと知的財産を守る。
- ＞ オートメーション・ネットワーク内のセンサーや機器を認証する。
- ＞ ソフトウェアやファームウェアのアップデートをセキュアに行い、知的財産を守り、操業の中断を防ぐ。

産業とセキュリティを融合する専門性と、個々の要求に見合うスケーラブルな製品ラインアップが、現代的なスマート工場を実現します。確立されたセキュリティのノウハウとインフラストラクチャを利用することで、セキュリティへの投資を抑制できます。



主なユース・ケース

OPTIGA™ のラインアップは、考えられる代表的なユース・ケースを網羅しています。

オーダーメイドの提案が行われる最も代表的なシナリオを以下に紹介します。



ソフトウェアやファームウェアのセキュアなアップデート

組込みシステムのソフトウェアやファームウェアは、定期的なアップデートが必要な場合が少なくありません。しかしながら、アップデート中のシステムだけでなく、ソフトウェアそのものを保護することは容易ではありません。ソフトウェアだけで対策を行ったアップデートでは、ソフトウェアを読み出し、解析して、アップデートやシステムに侵入できるように変更されるリスクがあります。しかし、セキュアなハードウェアと組み合わせることで、ソフトウェアを用いるものにできます。セキュアなハードウェア OPTIGA™ は、暗号化、異常および不正操作の検出、コードやデータのセキュアな保管により、コードの実行や保管を保護します。



保管データの暗号化と完全性の保護

組込みデバイスには、秘密のユーザ・データが保管されている場合があります。データの完全性と機密性は、暗号化や署名によって守ります。暗号鍵をセキュアに保管できるかが課題です。攻撃者が鍵を読み出せば、データを容易に復号化できてしまいます。OPTIGA™ Trust ファミリーや OPTIGA™ TPM ファミリーは、データを暗号化し、暗号鍵をセキュアに保管することにより、この課題を克服します。OPTIGA™ TPM はソフトウェアとハードウェアの完全性チェックもサポートします。



認証

ネットワーク上のユーザ、コンピュータ、機器や装置を識別し、許可された人や不正操作されていない機器にアクセスを限定する処理が認証です。ハードウェア方式のセキュリティは、機器の認証情報（暗号鍵やパスワード）にセキュアな保管場所を提供して認証をサポートします。機器やシステムのセキュアな認証を可能とするために、ハードウェア機器内にルート・オブ・トラストを設ける OPTIGA™ は、幅広い製品ラインアップを取り揃えています。



ブート・プロセス・プロテクション

セキュア・ブート、ベリファイド・ブート、トラステッド・ブートで知られるブート・アクセス・プロテクションは、コンピュータ機器の不正ブートをブロックし、感染デバイスがIoTを通じてデータを送ることを禁止します。ブート・プロテクションを強化し、完全性マトリックス管理の手間を省くために、インフィニオンは様々なセキュリティICを提供します。OPTIGA™ TPM は、トラステッド・コンピューティング・グループ(TCG)規格に準拠したブート・プロセス上のルート・オブ・トラストを実現します。



セキュアな通信

一般的な組込みシステム・アーキテクチャでは、様々な規格や独自プロトコルを採用した異なるネットワークを経由して、機器とシステムが接続されます。例えば、傍受やメッセージの改ざんから通信を保護するには、システム間をセキュアにしなくてはなりません。OPTIGA™ は、暗号処理をサポートするだけでなく、通信プロトコルで使用される鍵や証明書を保管することで、セキュアな通信を可能にします。

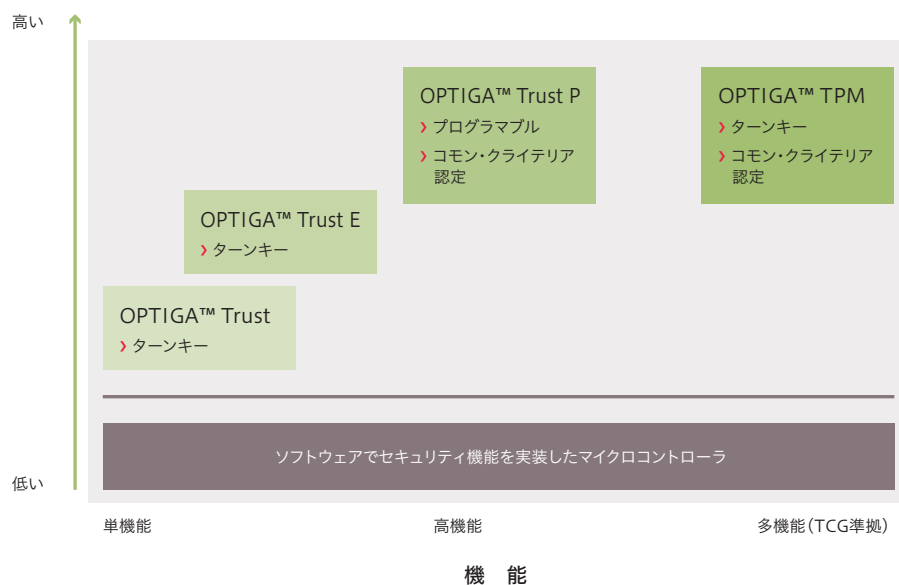


セキュリティの課題に応える OPTIGA™

セキュリティ・ソリューション OPTIGA™ は、組み込みシステムへ簡単に実装できるよう設計されています。このハードウェア方式のセキュリティ・ソリューションは、お客様ごとの様々なニーズに対応できるように、単純な認証から、複雑なものまで複数あり、

最大の投資効果が得られます。OPTIGA™ Trust ファミリーと OPTIGA™ TPM ファミリーのどちらも、信頼と実績のセキュリティ性能を発揮します。

セキュリティ・レベル



「OPTIGA™ Trust」ファミリー

組込みシステムのためのトラスト・アンカー

ターンキーもしくはプログラマブルなソリューションである OPTIGA™ Trust ファミリーは、ビジネス・モデル、製造ノウハウやIPの保護に最適なレベルのセキュリティを提供すると同時に、

簡単便利に実装できる特徴があります。OPTIGA™ Trust ファミリーは、偽造や模造、意図的な攻撃や思わぬ誤操作から組込みシステムを守ります。

OPTIGA™ Trust

組込みシステムのためのベーシックな認証ソリューション



OPTIGA™ Trust (SLS 10ERE)は、認証機能を簡単に実装したい組込みシステムのための、強固な暗号ソリューションです。OPTIGA™ Trust は、純正品の信ぴょう性や完全性、安全性を確保したいシステム・メーカーやデバイス・メーカー向けにデザインされています。

ターンキー・ソリューションの OPTIGA™ Trust は優れた模造品対策となり、OEMの信頼維持に役立ちます。

主な機能

- › ハードウェアで実現された先進の暗号アルゴリズム(163ビット楕円曲線暗号)
- › 簡単に実装できるホスト側ソフトウェアを含むターンキー・ソリューション
- › 3.5キロ・ビットのユーザ・メモリ
- › チップごとに異なる非対称の鍵ペア
- › PG-USON-3 小型パッケージ (2 x 3mm)
- › 簡単に使える単線ホスト・インターフェイス「SWI」

主な特長

- › 低コストのシングル・チップ・ソリューション
- › 非対称暗号とチップ個別の鍵による高いセキュリティ
- › 開発が容易なターンキー・デザイン

アプリケーション

- › IoT子機
- › プリンター・カートリッジ
- › 家電アクセサリ
- › 純正交換部品
- › 医療器具



OPTIGA™ Trust E

高性能システムのための簡単でリーズナブルなセキュリティ・ソリューション



OPTIGA™ Trust E (SLS 32A1A)は、システム側の実装をフルにサポートした、簡単でリーズナブルな高性能ターンキー型セキュリティ・モジュールです。OPTIGA™ Trust E は、サービスやビジネス・モデル、ユーザ・エクスペリエンスのプロテクションといった幅広い用途をサポートします。一方向認証機能が対象物を識別し、PKI（公開鍵基盤）ネットワークを守ります。

主な機能

- › 先進の暗号アルゴリズム(256ビット楕円曲線暗号)を採用した高性能ハードウェア・セキュリティ・モジュール
- › OSやアプレット、ホスト側の実装サポートを含むターンキー・ソリューション
- › I2Cインターフェイス
- › PG-USON-10パッケージ (3x3mm)
- › 最大3キロ・バイトのユーザ・メモリ
- › 標準動作温度モデル(−25~85°C)と、拡張動作温度モデル(−40~85°C)を用意
- › USBタイプCに最適

主な特長

- › 設計や開発の労力削減
- › IPやデータの保護
- › ビジネス・モデルやブランド・イメージの保護
- › 品質と安全性の保護

アプリケーション分野

- › IoTにつながる組込みシステム
- › 産業用制御機器、自動化機器
- › 医療機器、家庭電化製品
- › スマート・ホーム
- › PKIネットワーク



OPTIGA™ Trust P

組込みシステムのためのプログラマブル・トラスト・アンカー



OPTIGA™ Trust P (SLJ 52ACA)は、高性能かつ高機能なソリューションです。プログラマブルな OPTIGA™ Trust P は、鍵生成やアクセス制御を通して認証やセキュア・アップデートといった幅広い機能をサポートできる非常に柔軟で堅牢なソリューションです。このハードウェア・セキュリティ・モジュールは、サイドチャネル攻撃やフォルト誘導攻撃、物理的攻撃に対して先進的で効果的な防御を行います。

主な機能

- › 先進の暗号アルゴリズム (521ビット楕円曲線暗号、2048ビットRSA暗号、トリプルDES暗号、AES暗号)を採用した高性能ハードウェア・セキュリティ・モジュール
- › コモン・クライテリア EAL 5+ ハイ認定
- › 様々な用途に使えるサンプル・アプレットが付属したプログラマブルなJavaカードOSと、ホストのサポート
- › 150キロ・バイトのユーザ・メモリ
- › VQFN-32表面実装型パッケージ (5x5mm)
- › ISO/IEC7816 スマートカード・インターフェイス

主な特長

- › セキュアな認定ソリューション
- › 開発や実装を容易にするサンプル・アプレット付属のプログラマブル・ソリューションによる高い柔軟性
- › システムの整合性や通信、データの保護

アプリケーション

- › 産業用制御システム
- › 発電システム
- › 医療機器、ネットワーク機器
- › 家電製品
- › ホーム・セキュリティ、ホーム・オートメーション
- › IoTにつながる組込みシステム

OPTIGA™ TPM

標準化された高機能セキュリティ・ソリューション



TPM(トラステッド・プラットフォーム・モジュール)は、組み込みネットワークでのデバイスやシステムの整合性と信頼性を保護する、標準セキュリティ・モジュールです。実績あるTPM 1.2や最新規格TPM 2.0への対応により、OPTIGA™ TPM は、鍵や証明書、パスワード用のセキュア・ストレージに加えて、専用の鍵管理機能を取り入れています。

あらゆるニーズに応えるため、トラステッド・コンピューティング・グループ(TCG)規格に基づいて認定された多彩な OPTIGA™ TPM があります。

主な機能

- ▶ ハードウェアで実現された先進の暗号アルゴリズム(2048ビットRSA暗号、256ビット楕円曲線暗号、SHA-256など)を持つ高性能セキュリティ・モジュール
- ▶ コモン・クライテリア EAL 4+およびFIPSセキュリティ認定
- ▶ SPI、I2C、LPCインターフェイスのサポートによる柔軟な実装
- ▶ 様々なアプリケーションに使える拡張動作温度モデル(−40〜85°C)も選択可能
- ▶ 幅広いオープン・ソースのサポート

主な特長

- ▶ 規格化されたシステムのため低リスク
- ▶ 短期間での市場投入が可能
- ▶ 優れた鍵管理をはじめとする幅広いセキュリティ機能による柔軟性
- ▶ コンピュータ・プラットフォームへの実装が容易

アプリケーション

- ▶ PCおよび組み込み用コンピュータ
- ▶ ネットワーク機器
- ▶ 産業用制御システム
- ▶ ホーム・セキュリティ、ホーム・オートメーション
- ▶ 発送電システム
- ▶ 自動車用エレクトロニクス

「OPTIGA™ TPM」ファミリー概要

SLB 9645	SLB 9660	SLB 9665	SLB 9670
<ul style="list-style-type: none">▶ TPM 1.2▶ I2Cインターフェイス▶ コモンクライテリアEAL 4+認定	<ul style="list-style-type: none">▶ TPM 1.2▶ LPCインターフェイス▶ TCGおよびコモン・クライテリアEAL4+認定▶ FIPS 140-2認定(予定)	<ul style="list-style-type: none">▶ TPM 2.0▶ LPCインターフェイス▶ TCGおよびコモン・クライテリアEAL4+認定	<ul style="list-style-type: none">▶ TPM 1.2/2.0▶ SPIインターフェイス▶ TCGおよびコモン・クライテリアEAL4+認定

新規顧客を獲得できます

信頼できる実績のある認定製品が安心感をもたらし、新しいビジネスやサービスのモデルを生み出せます。

必要なものが見つかります

スケーラブルな OPTIGA™ なら、セキュリティ性能を組み込みシステムのニーズにぴったり合わせることができます。

信頼のアドバイザーが、 あなたのそばに

開発者にとってのインフィニオンは、組み込みセキュリティのニーズに関する信頼できるアドバイザーです。インフィニオンがパートナーになれば、広範な組み込みセキュリティの資産と専用のセキュリティ・インフラストラクチャをすぐに利用して、実装の手間を省き、時間と費用を節約し、貴重な資産や知的財産を守ることができます。

業界で最も広範で、最もスケーラブルな製品ラインアップに加えて、豊富なパートナー・エコシステム「インフィニオンセキュリティ・パートナー・ネットワーク (ISPN)」が持つコンサルティングの広大なグローバル・ネットワークとサポート経験を活用頂けます。インフィニオンのセキュリティ技術は、ビジネス・ケースの成功を手に入れるために役立つだけでなく、最終的には、セキュリティ上重要なアプリケーションでの絶好の新ビジネスやサービスのモデルを創出します。

www.infineon.com/ISPN



ニーズの変化に適應できます
オープン規格に基づいたオーダー・メイド・ソリューションが、成長に柔軟に對應します。

手間いらずです
セキュリティ・エコシステム全体に広がるインフィニ
オンの経験と専用インフラストラクチャが、実装作
業を簡素化、加速させます。

セキュリティへの投資を抑えます
標準化された設計により、実装作業を削減し、
市場投入までの貴重な時間を節約します。



モバイル版カタログ
iOSおよびAndroid向けアプリ

www.infineon.com/ccs
www.infineon.com/embedded-security

www.infineon.com/jp

Published by
Infineon Technologies AG
85579 Neubiberg, Germany

© 2016 Infineon Technologies AG.
All Rights Reserved.

Order Number: B189-I0281-V1-5A00-JP-EC-P
Date: 04/2016

Please note!

THIS DOCUMENT IS FOR INFORMATION PURPOSES ONLY AND ANY INFORMATION GIVEN HEREIN SHALL IN NO EVENT BE REGARDED AS A WARRANTY, GUARANTEE OR DESCRIPTION OF ANY FUNCTIONALITY, CONDITIONS AND/OR QUALITY OF OUR PRODUCTS OR ANY SUITABILITY FOR A PARTICULAR PURPOSE. WITH REGARD TO THE TECHNICAL SPECIFICATIONS OF OUR PRODUCTS, WE KINDLY ASK YOU TO REFER TO THE RELEVANT PRODUCT DATA SHEETS PROVIDED BY US. OUR CUSTOMERS AND THEIR TECHNICAL DEPARTMENTS ARE REQUIRED TO EVALUATE THE SUITABILITY OF OUR PRODUCTS FOR THE INTENDED APPLICATION.

WE RESERVE THE RIGHT TO CHANGE THIS DOCUMENT AND/OR THE INFORMATION GIVEN HEREIN AT ANY TIME.

Additional information

For further information on technologies, our products, the application of our products, delivery terms and conditions and/or prices please contact your nearest Infineon Technologies office (www.infineon.com).

Warnings

Due to technical requirements, our products may contain dangerous substances. For information on the types in question please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by us in a written document signed by authorized representatives of Infineon Technologies, our products may not be used in any life endangering applications, including but not limited to medical, nuclear, military, life critical or any other applications where a failure of the product or any consequences of the use thereof can result in personal injury.