暗号化なしでの
CAN通信の保護

NXP TJA115xセキュアCAN トランシーバ・ファミリ

NXP TJA115x CANおよびCAN FDトランシーバ・ファミリは、暗号化なしで従来のCANおよびCAN FD通信を保護するための、スムーズでコスト効果の高いソリューションを提供します。

概要

TJA115xトランシーバ・ファミリは、新世代の車載高速CAN/CAN FDトランシーバです。これらのトランシーバは、従来のCANまたはCAN FDプロトコル・コントローラと物理的な2線式CANバスをつなぐインターフェースとなり、暗号化なしでCAN通信の認証を提供します。セキュリティ・インシデントが検出されない限り、TJA115xトランシーバは標準的な高速CANトランシーバのように動作します。

各種のTJA115x製品は、標準SO8またはHVSON14パッケージで提供されます。

セキュアCANの仕組み

セキュリティ・インシデントが検出されると、TJA115xトランシーバがアクティブ・エラー・フレームを送信することにより、メッセージが無効化されます。これにより、このメッセージはどの受信バッファにも保存されなくなります。セキュリティ・インシデントの発生元がローカル・ホストである場合、 TJA115xトランシーバはそのローカル・ホストをCANバスから一時的に切り離します。

CAN IDやフィルタ設定のようなTJA115xトランシーバの設定は、検査ライン・プログラミングの一環として実施されます。設定は将来の現場でのセキュア・アップデートに向けてオープンにしておくことも、永久にロックすることもできます。

TJA115xトランシーバを使用することで、バス上でのセキュリティ・インシデントの記録とローカル・ホストへのレポートが容易になります。

主な特長

- 最大2 Mbit/sの高速CANおよびCAN FDのサポート
- SO8またはHVSON14パッケージで提供
- 現在の高速CANトランシーバとのフットプリント互換性
- 以下のセキュリティ・インシデントの検出と封じ込め：
  - Dos
  - 改ざん
  - なりすまし

- ローカル・ホストが、割り当てられていないIDでCANメッセージを送信しようとした
- ローカル・ホストのみに割り当てられているIDを含むCANメッセージを受信した

システムの価値と利点

システムへの影響を最小限に抑えた固有のセキュリティ・レベルの提供

TJA115xトランシーバを使用する際は、以下に挙げるシステム・アプリケーションの側面を考慮する必要があります。

- 従来のCANまたはCAN FDメッセージの正当な送信者であることの保証
- AUTOSAR®の「SecOC」やそれに似た機能の代わりにローカルCAN通信の認証に使用することで、以下の制約を除外
  - 帯域幅のオーバーヘッド
  - 暗号鍵の保管/処理の必要性
  - 起動遅延
  - レイテンシの増加
  - 追加のプロセッサ負荷
- 悪意のある、設定の更新からの保護
- （侵入）検知システム (IDS) での補完
- 侵入の即時封じ込め機能の提供

これらのセキュリティ機能は純粋にハードウェア・ベースの機能であるため、TJA115xはマイクロコントローラから完全に独立した状態で動作します。つまり、TJA115xトランシーバは固有のセキュリティ・レベルを提供するトランシーバであり、システムへの影響を最小限に抑えるとともに、CANプロトコル仕様における送信者識別の欠如を補えるよう特別に設計されています。

TJA115xトランシーバは、他のECUに影響を与えたり、メッセージのレイテンシやバス負荷に影響を与えたり、プロセッサ負荷を増大させたりすることなく、段階的に（ECUごとに）ネットワークに導入できます。

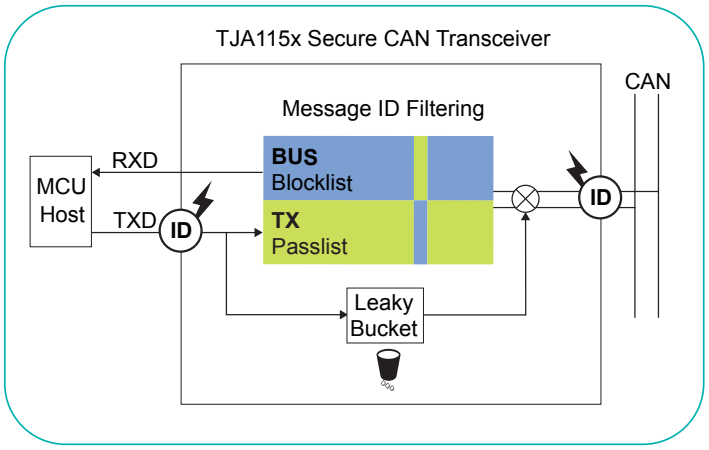
なりすまし保護

送信者に対するなりすまし保護のメカニズム（送信パスリストとバス・ブロックリスト）の実装により、対象のECU（メッセージ受信者）が保護対象のメッセージを受信したとき、 それが正しい送信者から送信されたメッセージであることを確認します。
また、CANバスで何らかの不審な挙動を検知すると、すぐにバスが保護されます。実装されているセキュリティ・メカニズムには、（個々のECUの）初期化や（バス上の複数のECUの）同期は必要ありません。

Dos攻撃保護

TJA115xトランシーバは、そのローカル・ホスト・コントローラから送信されるフレームの送信時間を測定します。測定した値は、累積バス負荷が設定可能な閾値を超えたときにオーバーフローする「リーキー・バケット」に追加されます。Dos攻撃は、アクティブ・エラー・フレームのあるメッセージの無効化と、セキュア・モードへの切り替えによ って通知され、ローカル・ホスト・コントローラがバスから切り離されます。Dos攻撃は、送信者が最大理論フレーム長よりも長くバスを確保しようとしたときにも検出されます。

TJA115xのアプリケーション原則



NXP TJA115xセキュアCANトランシーバ・ファミリ

Type	Package	Description
TJA1152AT	SO8	8-pin transceiver with Standby mode and V_{IO} pin
TJA1152BT	SO8	8-pin transceiver with Standby mode
TJA1153ATK	HVSON14	14-pin transceiver with Sleep mode and V_{IO} pin

改ざん保護

送信パスリストに従って認証されたローカル・ホストからの送信中に、TJA115xトランシーバはCANバス上の別のノードによって実行されたペイロードの変更を検出します。CAN仕様に従い、エラー・アクティブ状態では、ローカル・ホストのCANコントローラがそのような変更を検出し、処理します。ただし、エラー・パッシブ状態では、エラー・フレームによって変更が通知されることがなく、悪意のあるノードに改ざんの機会が残されることになります。改ざん保護が有効化されている場合、TJA115xは（セキュリティの観点から）エラー・パッシブ状態の時にペイロードの変更を検出すると、ローカル・ホストに代わってエラー・フレームを出力します。

標準的なCANからセキュアなCAN通信へのスムーズかつ簡単な移行

NXPセキュアCANトランシーバは、現在の標準的な高速CANトランシーバと置き換え可能な、セキュリティ機能付きハードウェアです。このトランシーバは、 ECUのハードウェア面やソフトウェア面の大きな変更を回避でき、他のECUの動作に影響を及ぼしません。このアプローチは、 迅速で必要な労力が少なく、コスト効果の高い方法でCANバスにセキュリティを導入するのに役立ち、スタンドアロンの保護メカニズムとして導入することも、さらに高度な、他のセキュリティ・ソリューションへの追加の防御層として導入することもできます。

www.nxp.jp/CAN

NXPおよびNXPのロゴは、NXP B.V.の商標です。その他すべての製品名、サービス名は、それぞれの所有者に帰属します。
All rights reserved. © 2020 NXP B.V.

ドキュメント番号： SECURCANTRLFUS REV 3