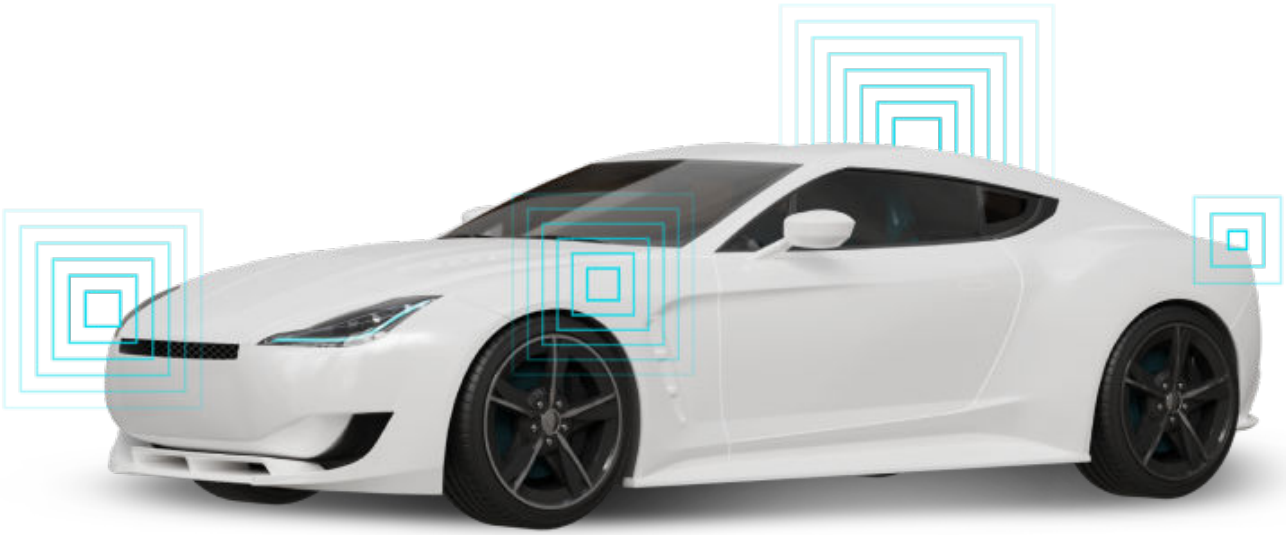
PLAXIDITYX

GO EVERYWHERE

A²Bセキュリティ：シンプルな
オーディオ伝送に隠れたサイバーリスク



執筆：

Robbie Galfrin、セキュリティリサーチャー

目次

概要

このホワイトペーパーでは、Automotive Audio Bus（A²B）プロトコルに関連するセキュリティ上の課題について検討します。A²BはAnalog Devices社が開発した高度な通信技術であり、1本の非シールドツイストペアケーブルを介して音声・センサー・制御データを伝送できる仕組みです。A²Bは効率性と柔軟性を大幅に高める一方で、リモートI²C（Inter-Integrated Circuit）通信の統合により、顕著なセキュリティリスクをもたらす可能性があります。これにより、ノード間での横方向移動（ラテラルムーブメント）、コンポーネントへの不正アクセス、さらにはECU（電子制御ユニット）の意図的な破壊といった攻撃が実現される恐れがあります。こうしたリスクに対抗するために、このホワイトペーパーでは具体的な緩和策を提案します。ハードウェア面では、I²Cバスの分離や専用サブチップの採用などの設計的対策を推奨し、ソフトウェア面では、外部入力データを非信頼データとして扱うこと、コードレビューの徹底、ファジングテストの実施といった安全策を提示します。これらの強固な緩和策を採用することで、自動車業界はA²Bの革新的な機能を最大限に活用しつつ、厳格なセキュリティ基準を維持することが可能となります。

はじめに

近年、自動車セキュリティは業界における最重要課題のひとつとして急速に注目を集めています。背景として、サイバー攻撃の増加と車両盗難などの物理的脅威という二重の圧力、それと同時に厳格な規制要件の推進があげられます。新しいインターフェースやコネクテッドシステムを車両に統合する技術的進歩は、利便性と機能性を大幅に向上させました。しかし同時に、それらの技術は攻撃対象領域を拡大させる結果にもなっています。新たなインターフェースが導入されるたびに、固有のリスクが生まれる恐れがあり、それらの脅威が意図せず持ち込まれないよう慎重に評価し、適切に管理することが求められます。この原則は、Automotive Audio Bus（A²B）にも当てはまります。

A²Bプロトコルは、Analog Devices社が開発した革新的な車載オーディオソリューションであり、車両全体にわたって音声および制御データを1本の非シールドツイストペアケーブルで伝送する、効率的な通信方式のことです[1]。A²Bは、他に類を見ない高い効率性と柔軟性を備えています。しかし、その実装においてリモートI²C（Inter-Integrated Circuit）通信を利用する場合、しばしば見落とされがちなセキュリティ上のリスクが生じる可能性があります。本ホワイトペーパーでは、これらのリスクを詳細に分析し、実践的かつ効果的な対策を提案します。

A²B概論

Analog Devices社が開発したA²Bプロトコルは、主に車載オーディオ用途を目的として設計されています[2]。しかし現在では、民生機器や産業オートメーションなど、他の分野でも採用が進みつつあります。A²Bは、複数のノードを単一のバス上に接続できるうえ、独立した電源ラインを必要としないため、システムアーキテクチャを大幅に簡素化し、全体のコスト削減にも寄与します。

A²Bテクノロジーの主なユースケースには、以下のようなものがあります。

- 先進運転支援システム（ADAS）、車両内での音声および制御信号の分配に利用
- ノイズキャンセリングシステム
- 分散マイクアレイ
- 産業オートメーション、工場設備などでのセンサー統合に応用

動作原理

A²Bネットワークは、1つのメインノードと複数のサブノードで構成される単一メイン・複数サブ（Single Main–Multiple Subordinates）トポロジを採用しています。このネットワークは主に、I²S／TDM または PDM 形式のオーディオストリームの伝送に使用されます。また、A²Bは複数の伝送方式をサポートしており、I²C-Over-DistanceプロトコルまたはA²B Mailboxを使用して、データおよび制御信号の送受信も行います。さらに、GPIO-Over-Distanceプロトコルにも対応しており、A²Bメインノードからサブノード側のA²Bトランシーバ上のGPIOピンを直接および遠隔制御が可能です。

通信は時間分割サイクル（time-divided cycles）で行われます。各サイクルは、まず A²B メイン から A²Bサブノード群 へデータが送信される下り方向のデータフレームと、次にチェーンの最下流に位置するA²BサブノードからA²Bメインに向けてデータが送信される上り方向のデータフレームの2つで構成されます。

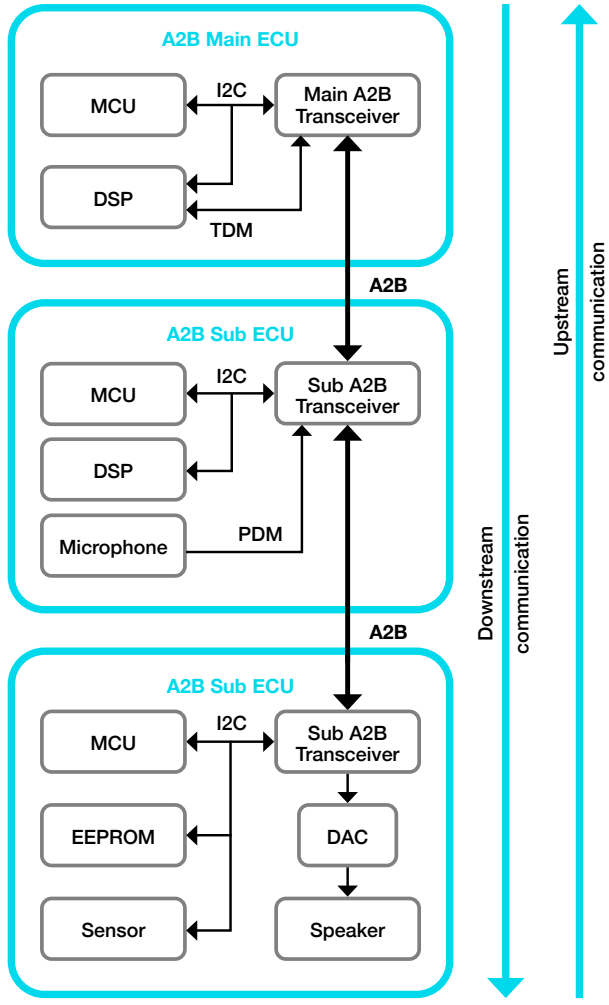


図1：A²Bバスの概要図

初期化の際、メインノードはネットワークの探索（discovery）および構成（configuration）を実行し、その結果ネットワークがアクティブな状態になります。ネットワークが確立されると、オーディオストリームが定義されます。これらのストリームは、動作開始前に静的に設定される場合もあれば、運用中に動的に設定される場合もあります。いずれの場合も、上りまたは下り方向のA²Bスーパーフレーム内でTDMスロット（Time Division Multiplexing slot）を割り当てることで、データ伝送の構造が決定されます。

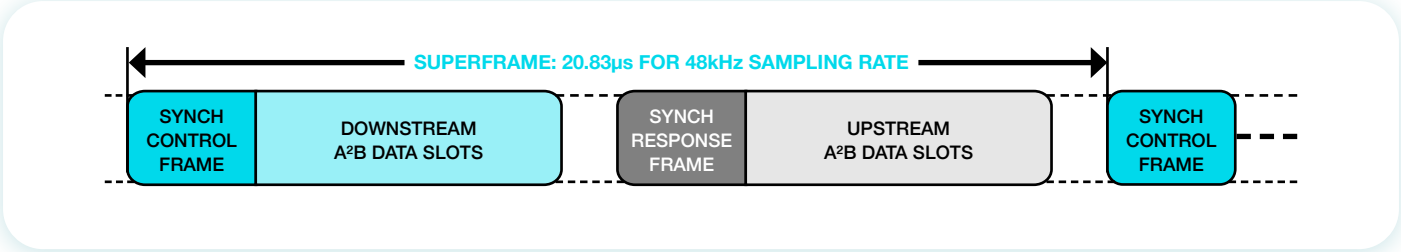


図2：A²Bスーパーフレーム構成。出典：AD242x reference manual [3]

その利点が明らかである一方で、A²Bプロトコル上でのリモートI²C通信は諸刃の剣でもあります。これは、新たな遠隔攻撃ベクトルを生み出す可能性があり、そのリスクは慎重に検討されるべきものです。

リモートI²C通信：基板レベル通信プロトコルの拡張

I²C-Over-Distanceは、A²B上でデータを転送するための仕組みであり、既存システムに容易に統合・インターフェース可能な形で設計されています。この方式では、標準的なI²C通信を透過的に遠隔実行できるようになっており、データはA²Bバス上のSYNCH制御フレーム（SYNCH control frames）の一部として転送されます。

この仕組みにより、A²Bメイン側のMCUは、サブノードの遠隔設定を行ったり、A²Bサブ側のMCUと通信したり、さらにはサブノード上のEEPROMメモリを直接書き換えたり、センサーを構成したりすることが可能になります。A²Bメインに接続されたホストMCUが、リモート側のA²Bサブに接続されたコンポーネントと通信する方法は2種類あり、それが I²C-Over-Distance と A²B Mailbox です。

I2C Over Distance

I²C-Over-Distanceでは、A²BチップがI²Cブリッジとして機能します。これにより、通信の両端にあるコンポーネントは、あたかも同一基板上の標準I²Cデバイスと通信しているかのように「思い込む」構造になっています。この方式は、A²Bメインノードに接続されたMCUが、A²Bサブノードに接続された周辺デバイス（I²Cサブデバイス）と通信するためによく利用されます。

たとえば、A²Bメインに接続されたMCUが、A²Bサブ上のセンサーからデータを読み取る、あるいはI²C EEPROMをプログラムする場合を考えます。このとき、メイン側のMCUはI²Cマスター（I²C Main）として動作し、その通信内容はA²Bバスを介して下り方向に転送され、対応するA²Bサブノードに届けられます。A²Bサブ側では、同様にI²Cマスターとして動作し、受信したメッセージを該当アドレスにミラーリングします。続いて、サブノード上のデバイスから返されたレスポンスは、A²Bバスを介して上り方向に送信され、A²Bメイン側に戻ります。メイン側ではこのときI²Cスレーブ（I²C Sub）として振る舞い、受信した応答をMCUにそのままミラーリングして返します。

A2B Mailboxes

A²B Mailboxは、軽量で非同期型の双方向メッセージパイプです。この仕組みでは、各ノードが1回の転送につき最大4バイトのデータを送受信することができ、割り込み（interrupt）を発生させると、相手側にI²C経由でMailboxの内容を読み取るよう通知します。

この方式は、A²Bバスの両端に接続されたMCU同士の通信によく使用されます。この通信は割り込みベースで動作します。送信側のMailboxへの書き込みが終わると、受信側に割込みが入ります。また、受信側の読み込みが終わると送信側に割り込みが入ります。この通信によって、通信を非同期的に実行することが可能です。割り込みが発生した際、各MCUはI²Cマスターとして動作し、Mailboxへの読み書きを行います。

各ノードにはそれぞれ2つのMailboxがあり、1つは受信（Rx）用、もう1つは送信（Tx）用として構成されています。MCUが相手側にデータを送信したい場合、まず送信Mailbox（Tx Mailbox）にデータを書き込み、その後、相手側で割り込み（interrupt）を発生させるためのレジスタ設定を行います。相手側のノードはこの割り込みを受信すると、任意のタイミングでMailboxの内容を読み取ることができます。データの読み取りが完了すると、受信側は送信元に対してデータを読み取ったことを通知し、送信側は次のデータフレームをMailboxに格納できるようになります。

A²B Mailbox通信スタック例

A²B Mailbox方式の利用に伴う潜在的なリスクをより正確に理解するために、ここでは一般的な通信スタック構造（communication stack）を詳しく見ていきましょう。

Mailboxレジスタは4バイトに制限されています。そのため、Mailboxをアプリケーション層（application layer）で意味のある通信に利用するためには、MCU上にトランスポート層（transport layer）を実装する必要があります。

そのような実装例のひとつを、以下の図に示します。

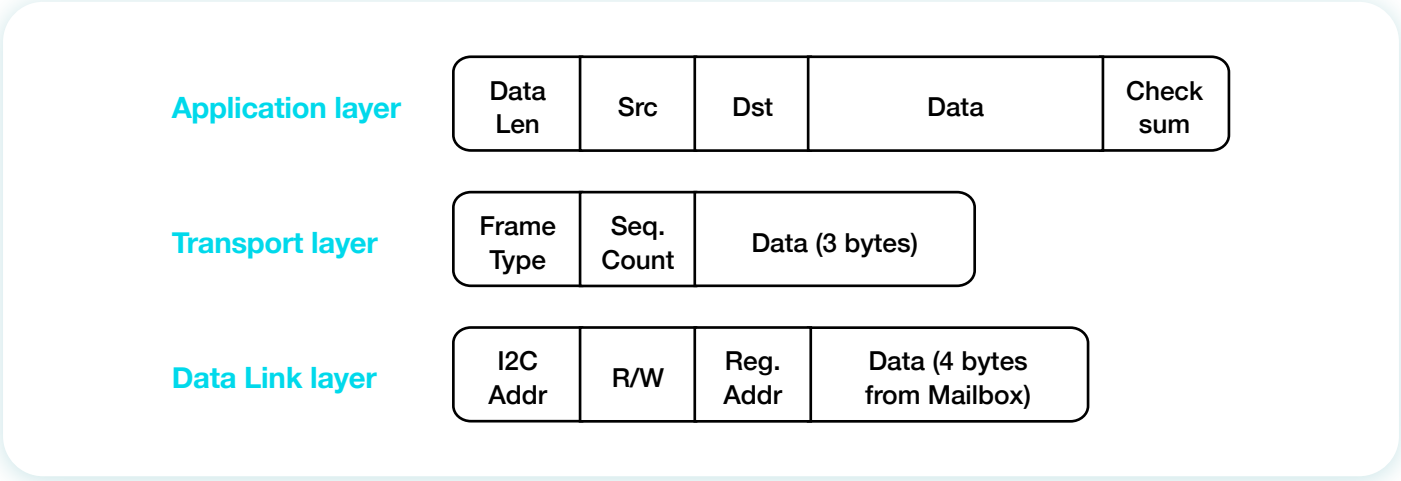


図3：MCU上におけるI²C Mailbox通信スタックの例

データリンク層（Data Link layer）は、Mailboxそのものに格納されているデータを指します。MCUはその上位にトランスポート層を実装し、Mailbox内の4バイト単位のデータを再構成（デフラグメント）して、より長いメッセージとして扱えるようにします。さらにその上にアプリケーション層を追加し、論理的な送信元・宛先の識別や、チェックサム（checksum）などによるデータ完全性の検証を行うことも可能です。

ここで重要なのは、このような実装はA²Bノードに接続されたMCU上で行われるものであり、A²Bプロトコル自体の機能ではないという点です。したがって、このような実装から生じるリスクはA²Bプロトコルそのものに内在するものではなく、むしろMCU上でのI²Cデータの処理方法に起因するものです。

つまり、発生しうる不具合や脆弱性はA²Bの仕様ではなく、MCU側のソフトウェア実装に依存するものとなります。

A²Bのセキュリティ脅威

A²BはI²C通信を遠隔で実行可能にするため、結果としてI²Cバスの範囲を単一の基板（PCB）の物理的境界を越えて拡張することになります。このことは、本来I²Cプロトコルが前提としていたセキュリティ境界を曖昧にし、新たなリスクを生み出す要因となります。これらのリスクは、システム設計時に慎重に検討すべき重要な課題です。

A²Bに関連する主要なセキュリティ脅威のひとつは、攻撃者がA²Bノードの制御を奪取した場合に、そのノードを足掛かりとしてA²Bネットワーク上の他のECUを侵害できてしまう可能性があることです。

以下は、ラテラルムーブメントを伴う潜在的な攻撃シナリオのいくつかの例です。

A²BメインECUから下流方向へのラテラルムーブメント

攻撃者がA²BメインのMCU上でコード実行能力を得た場合を考えてみましょう。そのような状況では、攻撃者はA²Bバスを利用して別のECUへアクセスを試みることが可能になります。

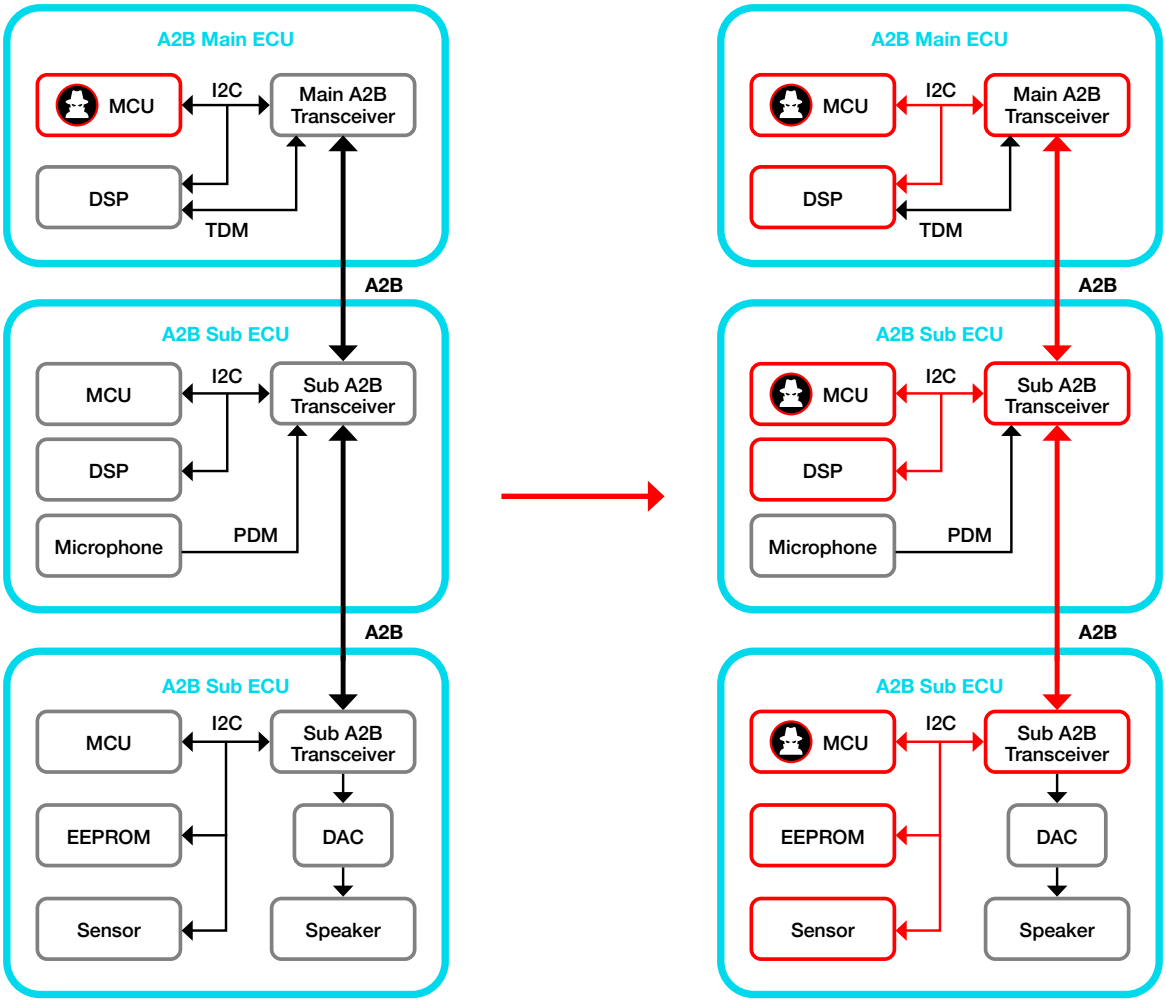
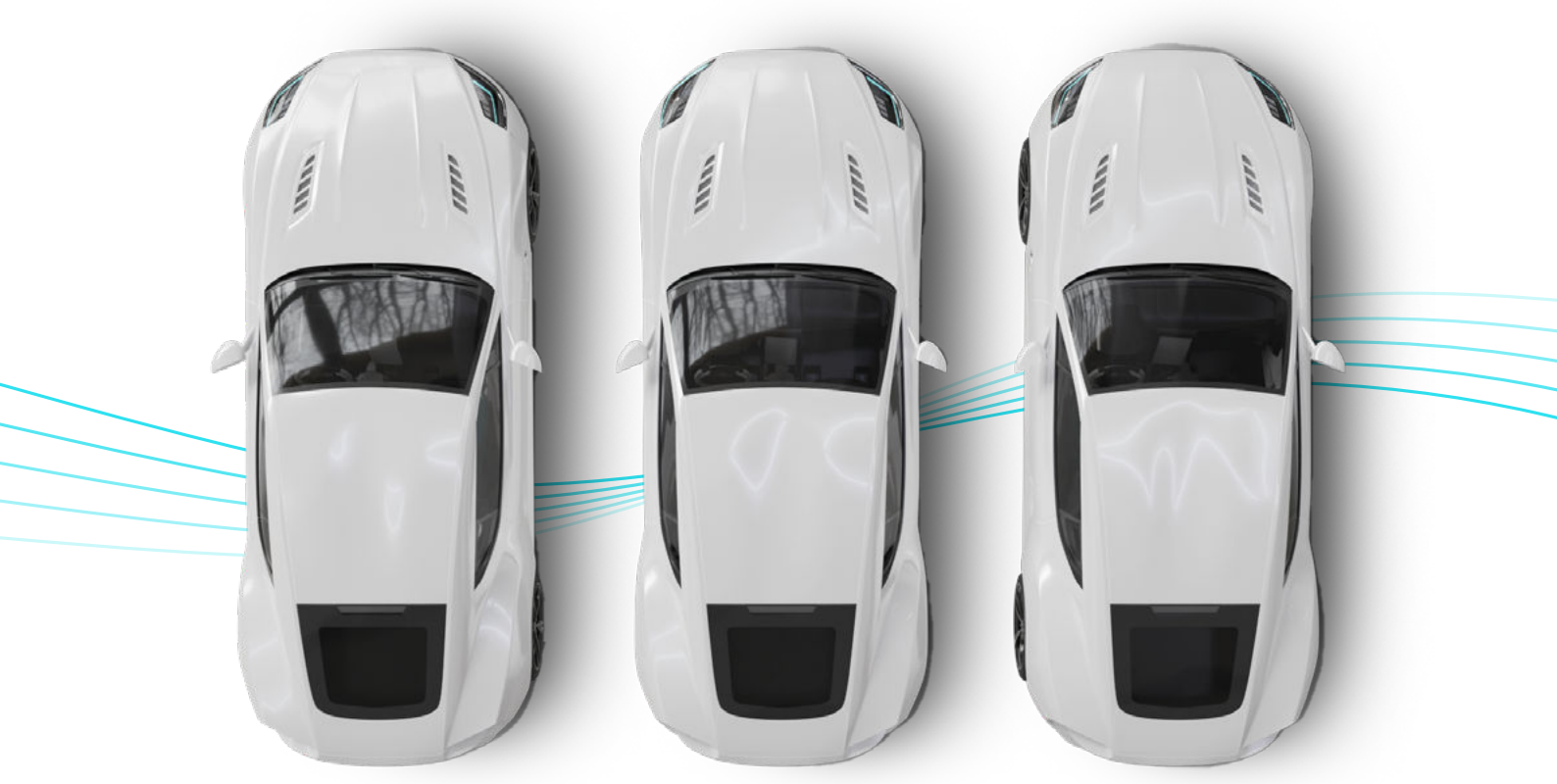


図4：侵害されたA²BメインMCUが下流のA²Bサブノードをさらに侵害するために用いられる例

考えられる攻撃ベクトルには、次のようなものが含まれる可能性があります。

- 攻撃者がA²Bメインを掌握している場合、バス上の任意のA²BサブにI²C通信を開始することが可能になります。例えば、A²Bサブ側のMCUがMailboxを用いた通信のためにトランスポート層やアプリケーション層を実装している場合、その実装中の脆弱性を攻撃者が突くことで、接続されたサブMCU上でリモートコード実行（RCE）を実行される危険があります。
- もう一つの潜在的な攻撃ベクトルは、A²BサブのI²Cバス上にある他のコンポーネントへの遠隔アクセスです。たとえば、A²BサブのMCUが同一のI²Cバスを用いてA²BトランシーバとEEPROMや各種センサーといった他の（直接関係しない）コンポーネントと通信していると仮定すると、攻撃者は遠隔でそれらと通信が行えます。具体的には、EEPROMのファームウェアを書き換える、センサーの設定を変更する、あるいはセンサー値を読み出すといった行為が可能になり得ます。
- さらに前述のとおり、GPIO-Over-DistanceによりA²Bメインはサブ側のPCB上にある物理的なGPIOを遠隔でトグル（オン／オフ切替）することが可能です。したがって、A²BサブECUのPCBレイアウト次第では、GPIOラインの電気的条件を悪用して故意に短絡を誘発し、サブをブリック化（起動不能化）したり、ECUに永久的なサービス妨害（パーマネントDoS）を引き起こしたりする恐れがあります。



A²Bサブノードの役割切り替え

一般的なA²Bチップはメインとサブの両方の役割が可能（例：AD2428、AD2430W、AD2437）であるため、攻撃者がA²Bサブ側のMCUを掌握すれば、そのA²Bチップをメインとして再構成することで、下流に接続されたすべてのA²Bノードを事実上制御できるようになります。

そのようなシナリオでは、攻撃者はサブ側のA²B DSPを掌握して、通常はDSPから発生するいくつかのA²B制御線、特にSYNCラインを再構成するかもしれません。

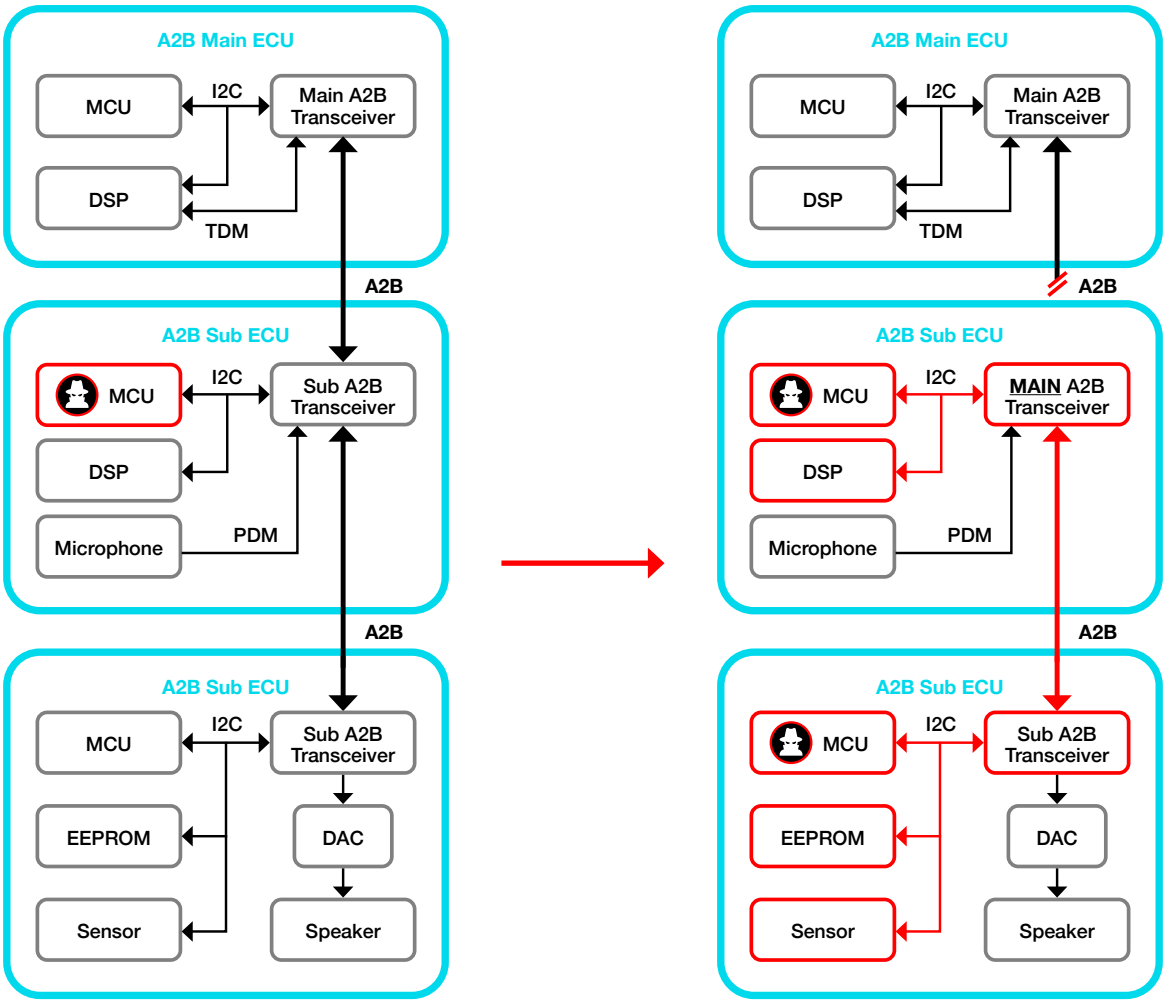


図5：侵害されたA²BサブノードMCUが下流の他のA²Bサブノードを侵害するために用いられる例

これにより、攻撃者はA²Bメインになりすますことが可能になり、前のセクションで説明したすべての攻撃を、侵害されたサブノードより下流に存在するすべてのA²BサブECUに対して実行できるようになります。

A²BサブECUから上流方向へのラテラルムーブメント

攻撃者がA²Bサブノードを侵害した場合には、上流方向へのラテラルムーブメントの可能性も併せて考慮する必要があります。

A²BメインとA²BサブのMCU間でI²C通信が行われる場合、A²BサブMCUはメインが開始したコマンドに対して応答を返します。そしてこれらのコマンドは、A²BメインMCU側の通信スタック上で処理されます。

したがって、攻撃者はA²BサブMCUからの応答を処理するA²BメインMCUのコードに存在する可能性のある脆弱性を悪用し、A²BメインMCU上でリモートコード実行を達成することがあり得ます。

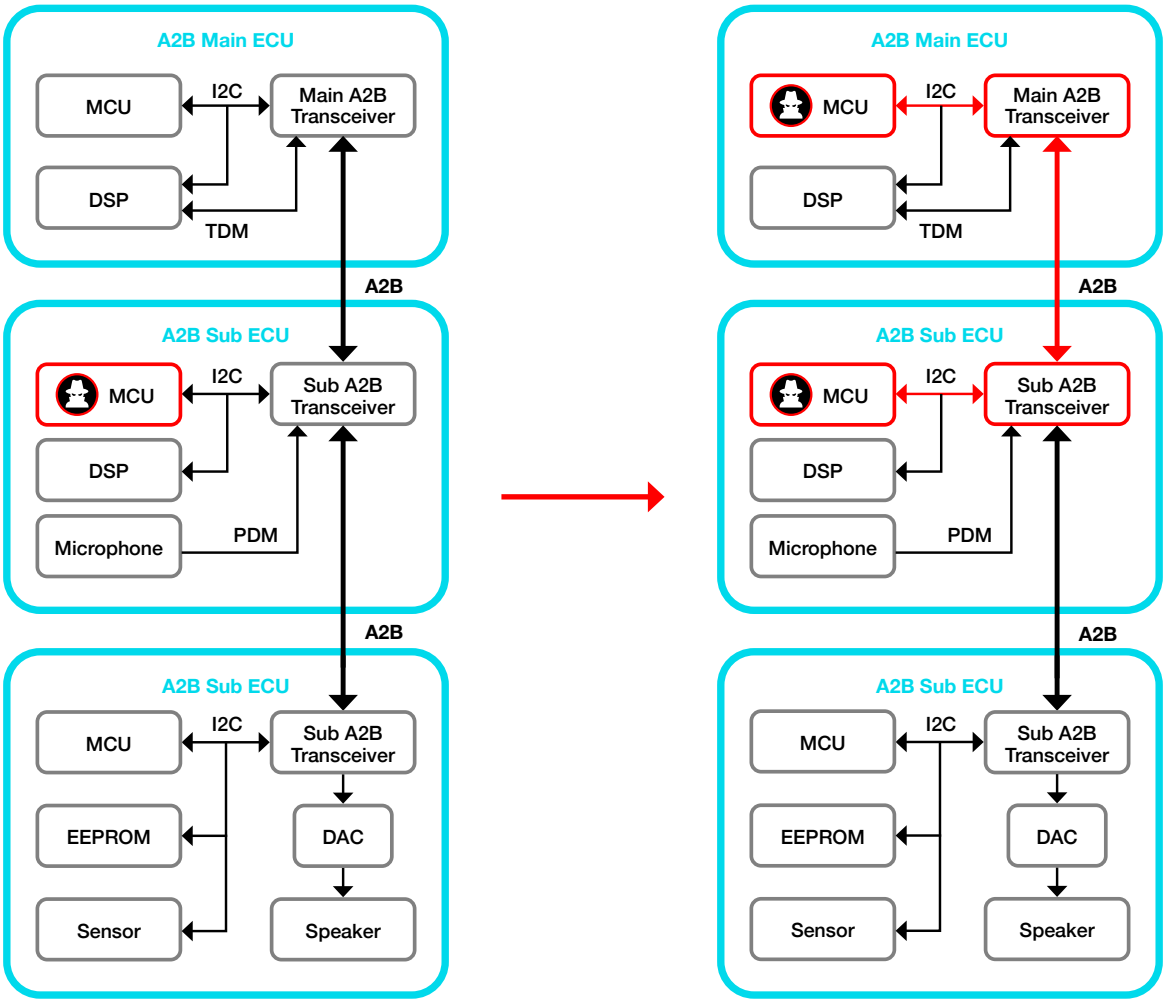


図6：侵害されたA²BサブノードMCUがA²BメインノードMCUを侵害するために用いられる例

緩和策と防御策

上記で説明した脅威を軽減するためには、ハードウェア設計レベルおよびソフトウェア開発レベルの両面から、いくつかの対策を講じることができます。

A²Bサブ ECUの実装

- ハードウェア設計の観点
  - A²B通信に使用するI²C物理バスを、他のコンポーネントで使用されるI²Cバスから分離し、A²Bメインが侵害された場合にリモートアクセスを防止できるようにします。
  - サブ専用のA²Bチップを使用し、攻撃者がそれをA²Bメインとして再構成できないようにします。
  - リモート制御されるGPIOのPCBレイアウトを確認し、GPIO方向（入力／出力）が不正に変更されることがないよう設計上の耐性を検証します。
- ソフトウェア実装の観点
  - A²BメインからくるI²C通信は非信頼（untrusted）入力として扱い、その取り扱いがMCUの侵害につながらないことを検証します。
  - このリスクを低減するためには、I²C通信スタックに対するセキュリティコードレビューを実施するか、あるいはA²Bインターフェースのファジングを行い、いかなる入力でもシステムが予期しない挙動をとらないことを確認することが有効です。こうした検証は、PlaxidityX AutoTester のようなインターフェース向けファジングツールを用いて実施できます。

A²Bメイン ECUの実装

- A²Bサブから到着するI²Cデータはすべて非信頼（untrusted）入力として扱い、その取り扱いがMCUの侵害につながらないことを必ず検証してください。リスク低減のためには、I²C通信スタックに対するセキュリティコードレビューを実施するか、あるいはファジングを行い、入力でもシステムが予期しない挙動をとらないことを確認することが有効です。こうした検証は、PlaxidityXが提供するようなインターフェース向けファジングサービスを用いて実施できます。

まとめ

A²Bプロトコルは、自動車オーディオシステムにおいて画期的なシンプルさと効率性を提供する一方で、リモートI²C通信を可能にする機能が新たな攻撃経路を生み出しています。自動車メーカーは、この脅威を通信スタック実装時のシステム全体のセキュリティ設計の一部として十分に考慮する必要があります。

A²B実装に関連するリスクには、A²Bバス上での上流・下流方向のラテラルムーブメント攻撃、共有リソースへの不正アクセス、さらには遠隔からの物理的損害などが含まれます。

しかし、適切な対策――たとえばI²Cバスの分離といったハードウェアレベルの防御や、厳格なソフトウェアテストを導入することで、これらのリスクを十分に軽減することが可能です。

システム設計段階からセキュリティ対策を優先することで、開発者はA²Bの革新的な機能を損なうことなく、車両セキュリティを確保することができます。

なお、このホワイトペーパーはAnalog Devices社のProduct Security Response Team（PSRT）と共有され、彼らのコメントを反映したうえで公開されています。

PlaxidityX サイバーセキュリティリサーチ&ソリューション部門について

PlaxidityX Cyber Security Research and Solutions部門は、自動車業界のサイバー防御をリードする存在です。車両アーキテクチャ、通信プロトコル、国際標準への深い理解を基盤に、当部門はクライアントに対して包括的なサイバーセキュリティサービスを提供しています。

当チームは、サイバーセキュリティと自動車分野の両方における専門知識を有しており、主要なOEMおよびTier1サプライヤーと連携しながら、数多くのペネトレーションテストおよびリサーチプロジェクトを実施してきました。その目的は、クライアントのサイバーセキュリティ体制を検証・強化し、UNR 155やISO/SAE 21434などの主要な業界規格への適合と、それを上回るレベルのセキュリティ実現を支援することにあります。

また、専用のリサーチプロジェクトから、先進的なPlaxidityX製品の導入支援に至るまで、当部門は常に進化する脅威に先んじるための実践的なソリューションと知見を提供しています。

参照

1. A2B Solutions by Analog Devices
2. An article about A2B Use Cases by Analog Devices
3. AD242X Reference Manual