

修士論文

意図的な電磁波照射による機器の入出力回路からの 情報漏えい制御に関する研究

碓 マーティン

2019 年 03 月 14 日

奈良先端科学技術大学院大学
情報科学研究科

本論文は奈良先端科学技術大学院大学情報科学研究科に
修士(工学) 授与の要件として提出した修士論文である。

裕 マーティン

審査委員：

林 優一 教授 (主指導教員)

藤川 和利 教授 (副指導教員)

安本 慶一 教授 (副指導教員)

藤本 大介 助教 (副指導教員)

意図的な電磁波照射による機器の入出力回路からの 情報漏えい制御に関する研究*

裕 マーティン

内容梗概

情報機器の物理層における脅威の一つとして、電磁波を介した情報漏えいの脅威がある。こうした脅威は、機器動作時に情報を含んだ電磁波 (漏えい電磁波) が非意図的なアンテナ構造を介して外部へ放射され、それを攻撃者が受信し、解析することで機器外部に情報が漏えいする。一方、従来このような脅威の対象は、情報を含む漏えい電磁波が設計者の意図に反して機器外部に放射される機器に限られていた。これに対し、本研究では、非意図的な電磁波放射が発生しない機器も対象となりうる新たな脅威について検討する。具体的には、通信線を介して接続された2台のマイクロコントローラを用い、それらに対して意図的な電磁照射を行うことで機器内部の入出力回路を構成する MOSFET を駆動し、ターゲットとなる信号を AM 変調することで、機器外部へ漏えいさせる。また、機器に照射する電磁波強度と機器外部に漏えいする電磁波強度の関係を実験的に明らかにし、これに基づき、上述した脅威への対策を検討する。

キーワード

電磁情報セキュリティ, 漏えい電磁波, 振幅変調, 電磁妨害

*奈良先端科学技術大学院大学 情報科学研究科 修士論文, 2019 年 03 月 14 日.

Study on inducing information leakage from input/output circuit inside device by intentional electromagnetic irradiation*

Martin Hazama

Abstract

One of the threats against the physical layer of information technology equipment/devices is information leakage through unintentional electromagnetic (EM) emissions from equipment. By measuring and analyzing these emissions, attackers can extract information from inside the equipment. On the other hand, some devices do not radiate EM emissions, and thus have been spared from conventional attacks. In this research, we will consider new threats targeting devices that do not radiate EM emissions. Specifically, EM fields are intentionally irradiated into the equipment, and EM fields including the internal information of the equipment are forcibly radiated by driving the MOSFETs constituting the input and output circuits of the equipment. This threat is shown by experiments using two microcontrollers. We also clarify the relationship between the intensity of irradiated EM fields and EM field intensity including the information, and discuss effective countermeasures against such attacks.

Keywords:

Electromagnetic information security, Electromagnetic leakage, Amplitude modulation, Electromagnetic interference

*Master's Thesis, Graduate School of Information Science, Nara Institute of Science and Technology, March 14, 2019.

目次

1. 序論	1
1.1 研究の背景	1
1.2 本研究の目的	2
1.3 本論文の構成	3
2. 漏えいの誘発手法とその対象	4
2.1 電磁波を介した情報漏えいのモデル	4
2.1.1 機器からの漏えい電磁波の発生原因	4
2.1.2 内部構造を用いた情報漏えいモデル	4
2.2 想定されるターゲットの概要	6
3. 漏えい情報の測定と評価	9
3.1 機器からの漏えい電磁波の測定	9
3.2 提案手法による漏えい電磁波の測定	12
3.3 照射強度による漏えい電磁波の増大の検討	15
3.3.1 電磁波の照射強度と側帯波の強度の関係	15
3.3.2 電磁波の照射強度と漏えい信号の類似度の評価	16
3.4 提案手法の脅威の考察	18
3.4.1 攻撃コストの考察	18
3.4.2 攻撃対象の範囲の考察	19
3.5 対策に関する検討	19
4. 結論	21
参考文献	23

1. 序論

1.1 研究の背景

2019 年現在、身の回りには多くの情報機器が存在し、個人情報をはじめとする重要な情報が取り扱われている。IoT 機器の普及により情報機器はさらに増加すると考えられている。そのため、情報セキュリティの重要性は更に増しており、様々なレベルで対策が検討、実施されている。情報機器は下位のレイヤを信頼して動作しているため、高いレベルのセキュリティ確保には、レイヤごとに対策を実施することが重要である。

その最下層のレイヤにあたる物理層での脅威の一つとして、電磁波を介した情報漏えいの脅威がある。情報機器は動作時に電磁波が放射することがあり、この電磁波に機器内部の処理情報が重畳した場合、外部からこの電磁波を測定、解析することにより内部情報が漏えいすることがある。電磁波による情報漏えいの脅威については、以前から検討が行われており、学術分野では 1980 年代に論文による報告がなされている [1]。しかし、当時は使用する装置が大変高価で大規模なものであったため、軍事外交レベルでの検討が主で、民間レベルでは大きな脅威と認識されていなかった。しかし近年、測定機器の低価格化、高性能化により、ディスプレイ、キーボード、プリンタなど一般的な機器に対する攻撃が報告されており [2][3][4]、民間レベルでも現実的な脅威として認識されている。

こうした脅威の原因となる機器からの電磁波放射のメカニズムは、電磁環境両立性 (EMC : Electromagnetic Compatibility) の分野では Source-Path-Antenna の三つの要因モデルで説明されている。Source とは情報システム内部の電気信号であり、この信号が Path と呼ばれる設計者の意図しない電氣的、磁氣的結合により、Antenna として振る舞う基板上の回路パターンや周辺配線へと伝搬し、信号を含んだ電磁波として外部に放射される。これらの各要素は、回路構造、筐体の材質、形状など機器の電磁氣的特性に依存するため、同じ用途の機器であっても機種によって漏えい電磁波の強度は異なる。また機器からの不要電磁放射 (エミッション) は他の機器の動作の妨害を防ぐことを目的として規制が設けられているが、規制に準拠した機器であっても漏えい電磁波から情報が漏えいしてしまうこ

とが報告されており [5]、従来の EMC 基準では十分でないことが示唆されている。

機器から放射される漏えい電磁波の強度が強い機器は弱い機器と比較した時、より遠方まで電磁波が伝搬するため情報漏えいが発生しやすい。一方で放射が機器外部から観測できない機器では情報漏えいが発生しないため、脅威の対象外となる。このように放射強度が情報漏えいのしやすさに大きく関係しているため、対策は漏えい電磁波の強度を減衰させることに重点を置いている。

従来の電磁波を介した情報漏えいに対する対策は、ゾーニングと呼ばれる漏えい電磁波の信号雑音比 (signal-noise ratio:SNR) を低下させ、情報を復元させない試みが行われている [6][7]。これは、機器本体、機器が動作する部屋、機器が動作する建物、建物の周囲の管理可能な区域のようにゾーンを設定し、ゾーンごとに対策を行い、攻撃者が接近可能な距離での漏えい電磁波の受信を防ぐことを目的としている。機器本体に対する対策では、機器のシールドやケーブルへの放射電磁波を低減する対策や、人為的にノイズを生成し、マスキングする対策などがある。部屋や建物に対する対策は、構造レベルで電磁波が伝搬しにくくする対策や、壁面や天井などのシールディングなどが挙げられる。

こうした対策は機器からの漏えい強度が基本的に一定で変化しないことを前提としている。しかし、攻撃者が漏えいの強度を制御することが可能であれば、元来機器からの漏えい電磁波が微小な機器や、対策が施された機器が情報漏えいの脅威に曝されることとなり、より重大な脅威となる。

1.2 本研究の目的

上述の背景をふまえ、本研究では攻撃者が機器の内部構造を利用することで、機器の漏えい電磁波の強度を制御する手法について提案を行う。また、こうした脅威の対象となると考えられるターゲットを模擬した環境を構築し、実験を通じて漏えい電磁波の強度の制御が可能であることを示す。

1.3 本論文の構成

本論文の構成は以下の通りである。

第2章では、従来の漏えいパラメタが決定されるメカニズムについて説明し、提案手法のアプローチとそれを実現できる回路構造を示す。また、実験環境として、相互に接続される情報機器を想定し、2台のマイクロコントローラが伝送路を通じてシリアル通信を行う環境を提案し、提案手法を実現できる構造が存在しているかの検討を行う。

第3章では、第2章で作成した実験環境を用いて、マイクロコントローラ間の通信信号をターゲットとして、漏えい電磁波を介した情報漏えいの検討を行う。従来の機器からの漏えい電磁波から取得した波形と、提案手法での取得波形を比較し、機器に実装された回路により、情報漏えいが発生していることを示す。また、漏えい電磁波の強度を制御可能であることを、機器への照射強度をパラメタとして、漏えい電磁波の強度の変化や、復元信号のターゲット信号との類似性を用いて評価を行う。

第4章では、本論文のまとめを行う。

2. 漏えいの誘発手法とその対象

2.1 電磁波を介した情報漏えいのモデル

本節では、機器からの漏えい電磁波の発生と漏えいパラメタが決定される原理を説明し、提案手法でのアプローチを示す。また、提案手法を実現する機器内部の構造を示す。

2.1.1 機器からの漏えい電磁波の発生原因

多くのデジタル回路において信号レベルの High から Low、Low から High への切り替えは、IC 内部の MOSFET がスイッチングによって行われている。このスイッチングの際、一瞬だけ電源－グラウンド間が短絡された状態になり、貫通電流と呼ばれる電流が流れる。これにより情報信号の切り替わり時に高調波が発生する。この高調波が設計者の意図しない結合を経て、非意図的なアンテナとして振る舞う部分から外部へ放射される。このように機器外部へ放射された電磁波を攻撃者が受信し、情報を再構築することにより情報が漏えいする。

この際の放射パラメタ (周波数、強度) は図 2.1 に示すように、発生した高調波と SPA モデルの Path と Antenna の周波数特性で決定される。Path や Antenna の特性は機器の様々な条件に影響されるため、推定が困難である。そのため、機器からの漏えいが最も強くなる周波数は偶発的に決定される。そのため機器からの漏えい電磁波のパラメタは必ずしも、効率の良い放射の条件を満たすとは限らない。

2.1.2 内部構造を用いた情報漏えいモデル

そこで本研究では、攻撃者の干渉により、Path-Antenna の特性上効率よく伝送可能な周波数で漏えいを誘発させることで、より強い漏えいを発生させる手法について提案を行う。選択的に漏えいを発生させる手法として振幅変調を用いる。攻撃者が機器外部から所望の周波数の搬送波を機器に注入し、機器内部で振幅変

調を行い生成された振幅変調波を機器外部へ放射させることで、搬送波の周波数を中心とした漏えいが発生する。

図 2.2 に機器内部に存在しうる提案手法を実現する構造を示す。この回路は MOSFET と非意図的なアンテナで構成される。非意図的なアンテナ構造から、信号の注入、生成された振幅変調信号の放射を行う。MOSFET ではゲートがターゲット信号の流れる線路へ接続されており、ターゲット信号の振幅によりソースドレイン間の抵抗値が変化する。電磁波の照射により、外部から注入された搬送波信号が、ソースドレイン間抵抗値の変化により振幅変調され、振幅変調波が生成される。

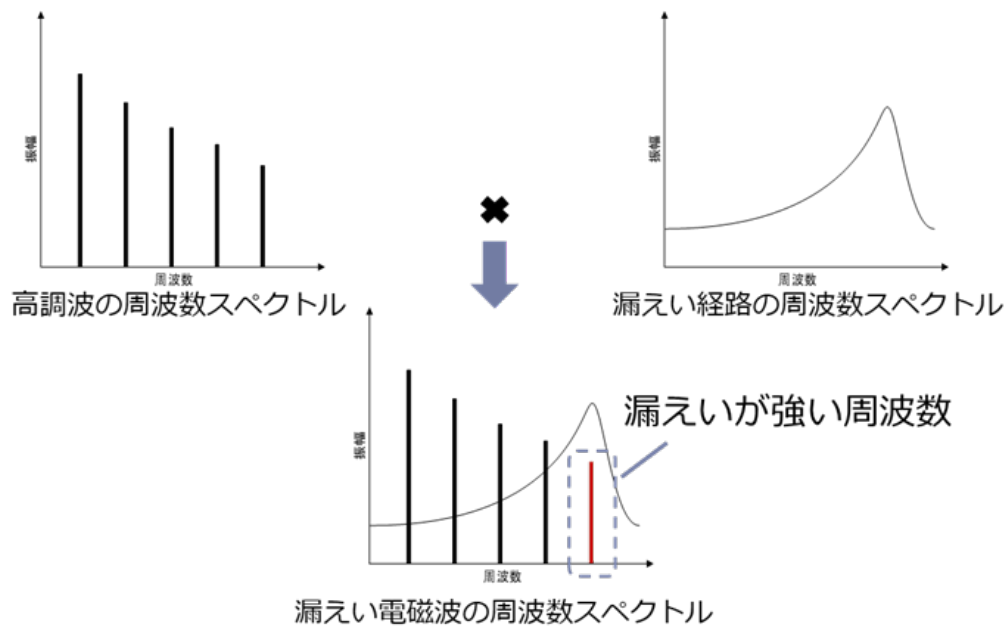


図 2.1 漏えい電磁波の発生モデル

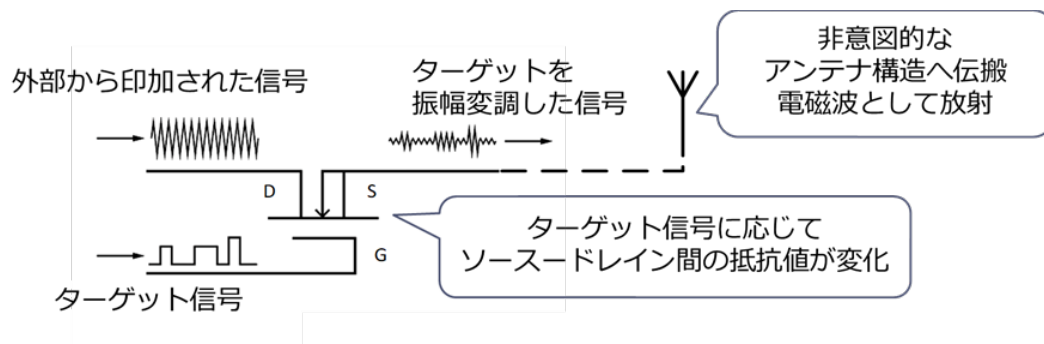


図 2.2 漏えいを誘発する構造

2.2 想定されるターゲットの概要

本研究では汎用的な通信に用いられるマイクロコントローラによる通信環境を模擬する。図2.3に示すように、2台のマイクロコントローラ (CY8C4245AXI-483) を、マイクロコントローラでの通信に一般的に用いられるツイステッドペアケーブルで接続し、一方から他方へシリアル通信 ('1','0' を電圧の High/Low で伝送) を行っている。この信号をターゲット信号として通信を行う。信号の周波数は、マイクロコントローラの正規のツールで設定可能な範囲内であれば、MOSFETの動作可能な範囲内の周波数となるため、攻撃が可能であると考えられる。そのため、本論文の実験においては、測定機器のスペックを考慮し信号を設定する。

ターゲットに MOSFET が実装されていることを確認する方法として、オンライン上に公開されているデータシートが挙げられる。本研究でターゲットとなるマイクロコントローラ (CY8C4245AXI-483) のデータシートを図 2.4 に示す [8]。このように攻撃者は公開情報から、攻撃可能な機器を調査することが可能である。また、このようなデータシートが公開されていない機器に対しても、機器の基本構造は共通であると考えられるため、他の機種の情報収集することにより漏えいを誘発する構造を推定することが可能である。

また、ターゲットとして用いるマイクロコントローラには、信号を出力しているピン以外にも多くのピンがありそれらも同様な漏えいを引き起こす構造が存在

していると考えられる。本研究でのターゲットの構成では、信号が出力されているピンにのみ通信線が接続されているため、非意図的なアンテナ特性が他のピンと比較して大きく異なると考えられる。そのため通信線が接続されているピンのアンテナ特性を推定することで、ターゲットのピンへ効率よく信号を注入できると考えられる。



図 2.3 ターゲットの概観

Figure 7-2. I/O Cell Architecture in PSoC 4100/4200

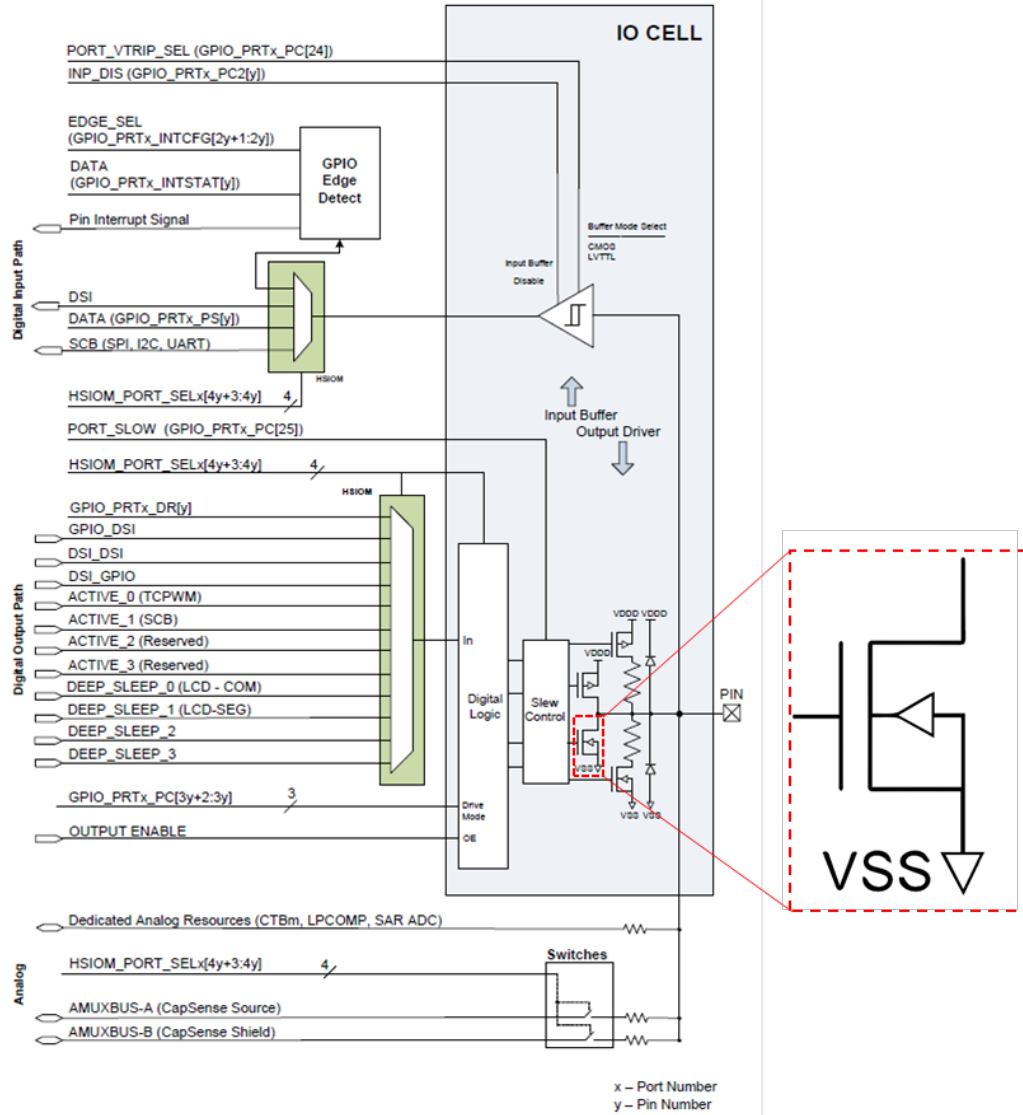


図 2.4 CY8C4245AXI-483 データシート [8]

3. 漏えい情報の測定と評価

3.1 機器からの漏えい電磁波の測定

非意図的なアンテナを介して機器からの漏えい電磁波の放射が発生している周波数では、電磁波の相反性により漏えいとは逆の伝搬方向で電磁波を注入できる可能性がある。本節では、提案手法でのターゲットへの電磁波照射により効果的な注入が行える周波数を決定するために、機器からの漏えい電磁波の測定を行う。

想定される情報漏えいの経路を図3.1に示す。2.1.1節で述べたように、MOSFETのスイッチングにより発生したノイズ(高調波)が通信線路へ伝搬し、空間へ放射される。放射された漏えい電磁波が最も強い周波数を測定することで、この経路で最も効率よく伝送できる周波数を推定する。

測定セットアップを図3.2に示す。木製テーブルに置かれたターゲットは一方から他方へ、図3.3に示すような信号を送信している。送信時に発生する漏えい電磁波をターゲットから3m離れた受信アンテナで受信する。攻撃を行う前に、漏えいが強い周波数の測定を行った。スペクトラムアナライザを用いて、受信アンテナの帯域内である430MHzから800MHzの周波数スペクトルを測定し、マイクロコントローラの非動作時の背景ノイズとの差分をとることにより機器の放射が測定できる。本研究の実験環境では機器からの漏えい電磁波が微弱であったためか、目視でスペクトルを確認できなかったため、35dBのアンプを用いてアンテナ感度を増幅した。

スペクトラムアナライザによる測定の結果、受信強度が最大となる周波数は557MHzであった。次に、この周波数でソフトウェア無線(Software-defined radio:SDR)を用いて受信、振幅復調を行った結果を図3.4に示す。図3.3のオリジナル信号の遷移と同じ間隔でスパイク状の波形が観測されたため、通信信号が電磁波として漏えいしていることが確認できた。

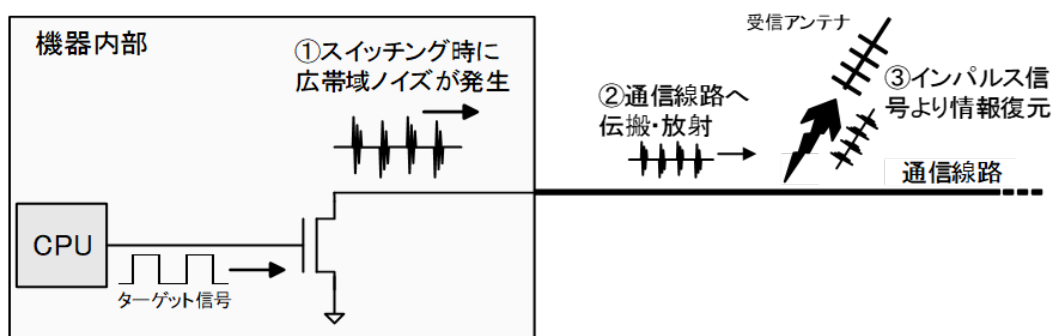


図 3.1 機器の情報信号の電磁波による漏えい経路

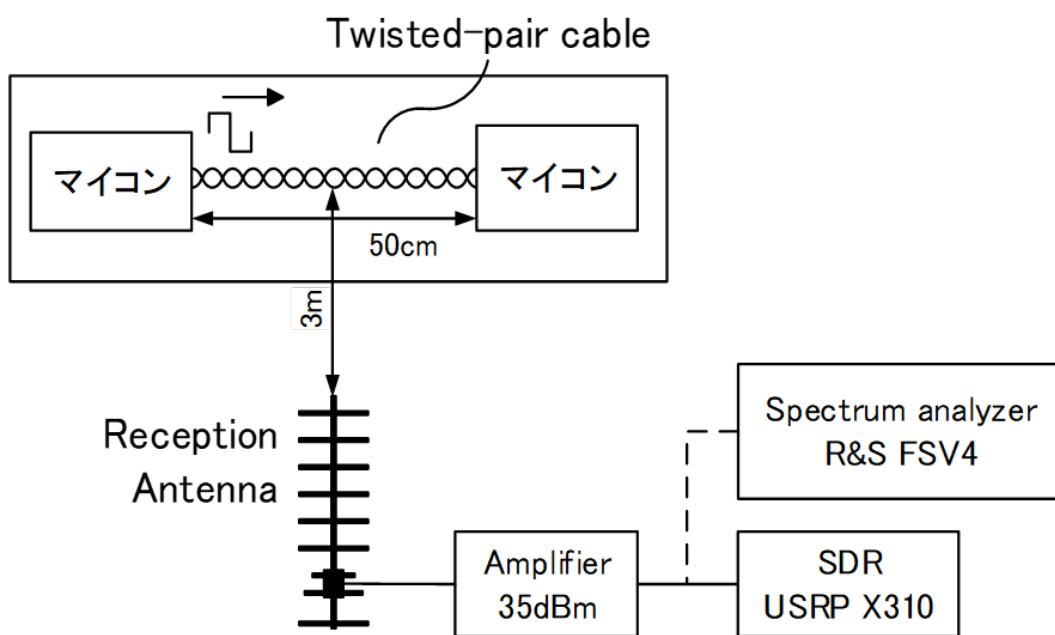


図 3.2 機器からの漏えい電磁波の測定セットアップ

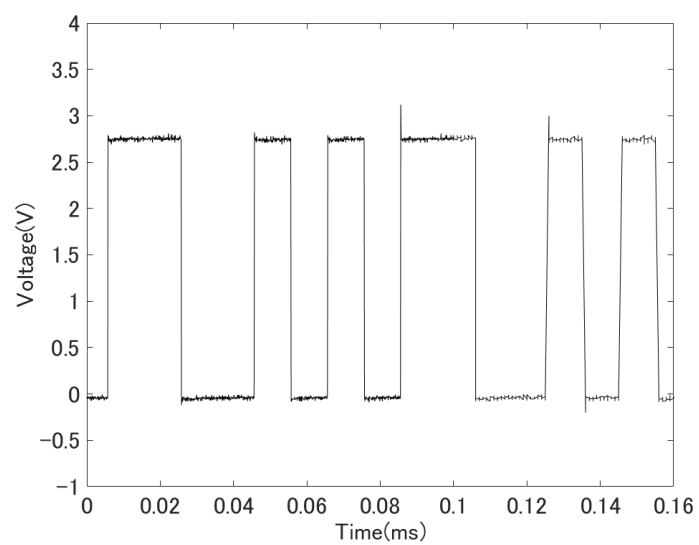


図 3.3 マイクロコントローラ通信波形

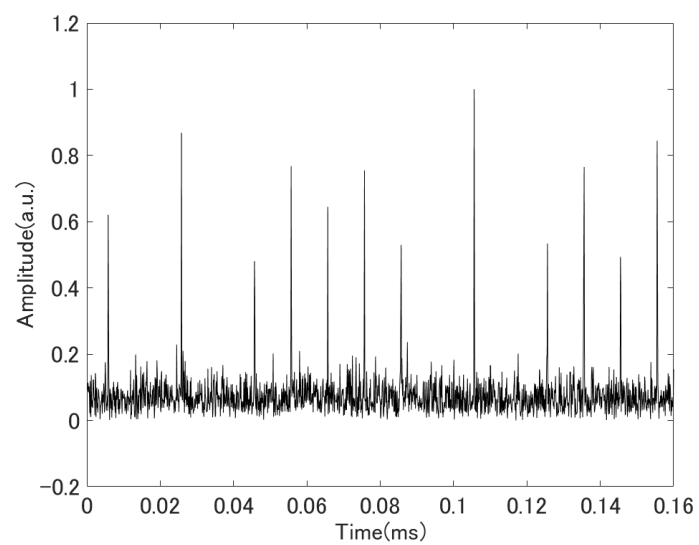


図 3.4 機器からの漏えい電磁波に含まれた漏えい情報

3.2 提案手法による漏えい電磁波の測定

提案手法での漏えい経路を図 3.5 に示す。3.1 節の結果から、漏えい電磁波が最も強く放射されていた 557MHz で電磁波を照射することにより、図 3.1 とは逆の方向で搬送波の注入が可能であると考えられる。

提案手法でのセットアップを図 3.6 に示す。ターゲット信号は 3.1 節の構成と同様である。シグナルジェネレータで搬送波として注入する正弦波を生成し送信アンテナからターゲットへ照射する。3.1 節での結果から、最もターゲットへ効率よく信号を注入できる周波数は 557MHz であった。

照射時に発生する側帯波を中心として、振幅復調した結果を図 3.7 に示す。遷移のタイミングにスパイク状の波形が現れる機器からの漏えいとは異なり、ターゲットの信号に忠実な波形が取得できた。一方電磁照射を行わないときは、図 3.8 の様に漏えいが発生しない。このことから 2.1.2 節で仮定したモデルと同様に、電磁照射による信号注入により漏えいが発生していることが確認できた。

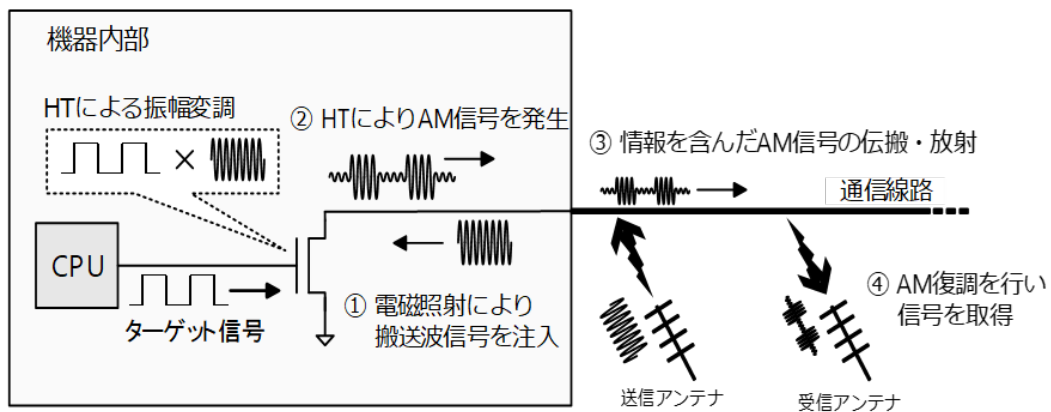


図 3.5 提案手法での漏えい経路

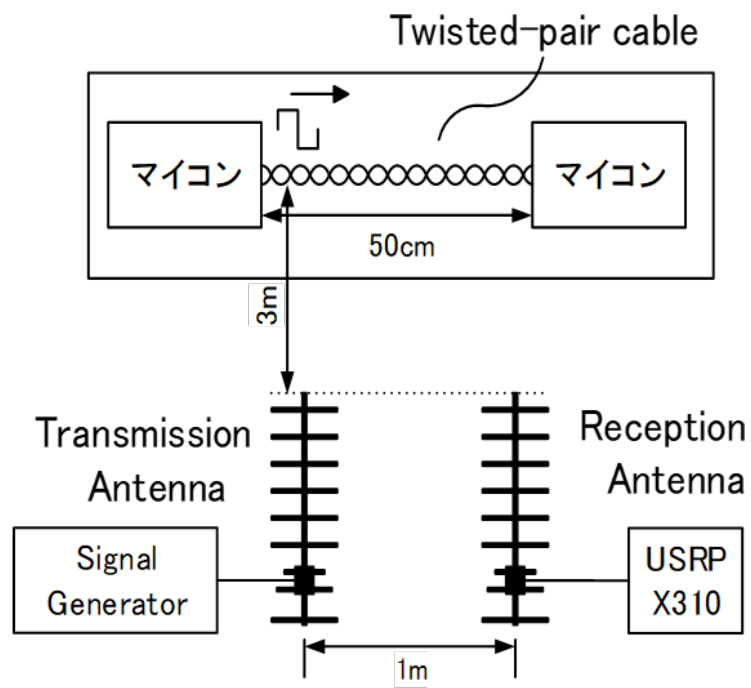


図 3.6 提案手法での測定セットアップ

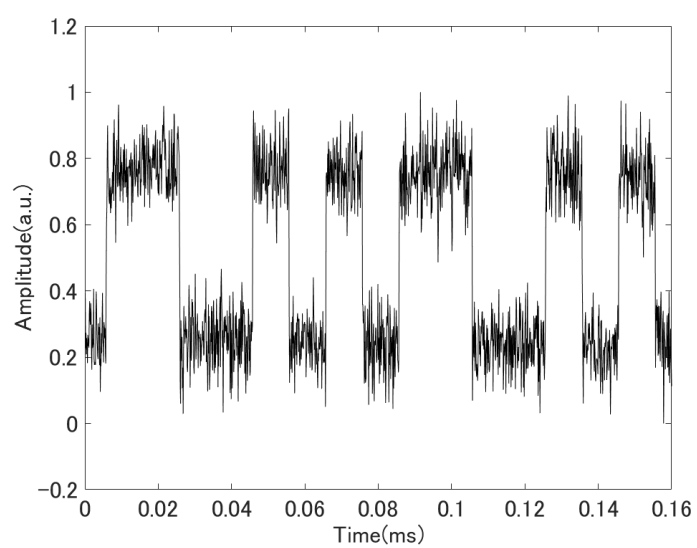


図 3.7 電磁波照射時の漏えい情報

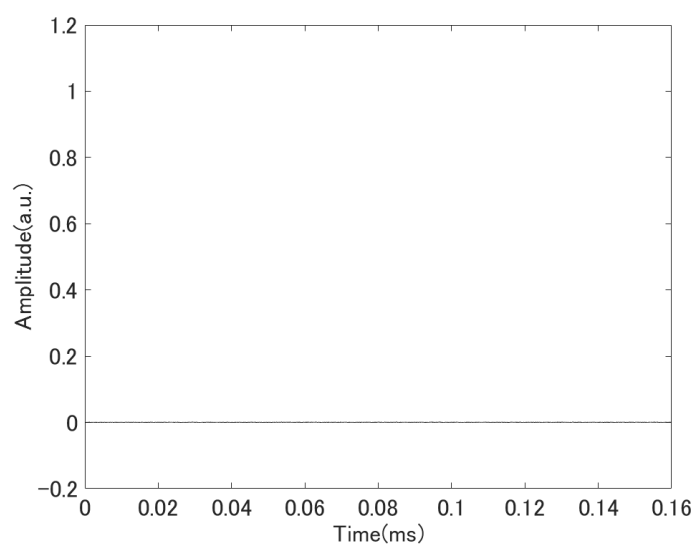


図 3.8 電磁波非照射時の漏えい情報

3.3 照射強度による漏えい電磁波の増大の検討

提案手法では、機器への照射強度に応じて、機器から放射される漏えい電磁波の強度が変化する。MOSFET の許容範囲内では、注入する搬送波の振幅が強いほど、漏えい電磁波の強度が増大すると考えられる。電磁照射の強度が強いほど、長距離の伝搬による減衰を経てもノイズに埋もれることなく信号が復元可能となる。

本節では、照射強度パラメタとして、漏えい電磁波の強度、復調信号とターゲット信号との類似度の測定することにより、照射強度を変化させることによる攻撃可能な距離の変化を評価する。

3.3.1 電磁波の照射強度と側帯波の強度の関係

はじめに、電磁照射の強度と側帯波の振幅についての測定を行った。測定セットアップの、ターゲット、送信アンテナ側の構成は図 3.6 同様である。ノイズや減衰による測定への影響を低減するため、ターゲットとの距離は 1m とした。受信アンテナ側には、定量的に強度を測定するためにスペクトラムアナライザを用い、側帯波の振幅を 100 回測定した平均値を記録した。測定結果を図 3.9 に示す。結果から、照射強度と側帯波のピーク強度は比例関係にあることが分かる。

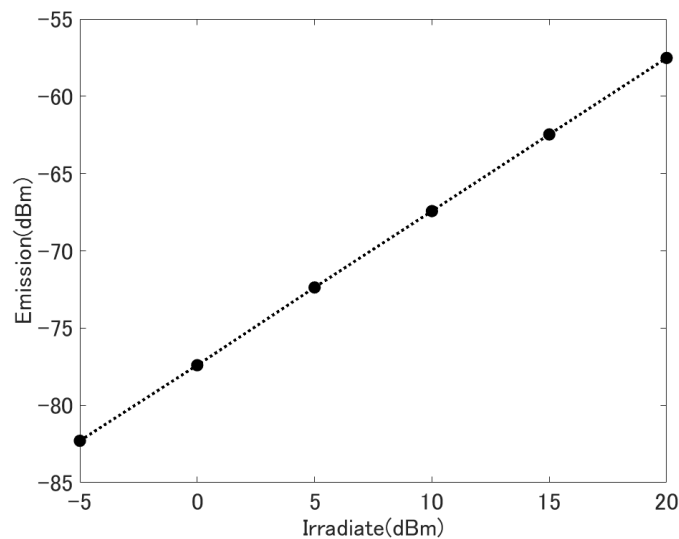


図 3.9 照射強度と側帯波の振幅の関係

3.3.2 電磁波の照射強度と漏えい信号の類似度の評価

次に、照射強度に対する漏えいの強さの評価を行う。図 3.10 のような波形をターゲットとして、図 3.6 のセットアップで測定を行った。また、側帯波の強度測定と比較を行う為、ターゲットとの距離は 1m とした。類似度の評価には相互相関を用いた。照射強度ごとの相互相関の最大値をプロットした結果を図 3.11 に示す。こちらも側帯波のピークと同様に、照射強度が増大すると、相互相関の最大値が増大し、よりターゲット信号に忠実な漏えい電磁波が発生することが分かる。このように照射強度を増大させることにより、漏えい電磁波の強度が増大し、より遠方からでも減衰によりノイズに埋もれることなく、漏えい電磁波を受信できると考えられる。

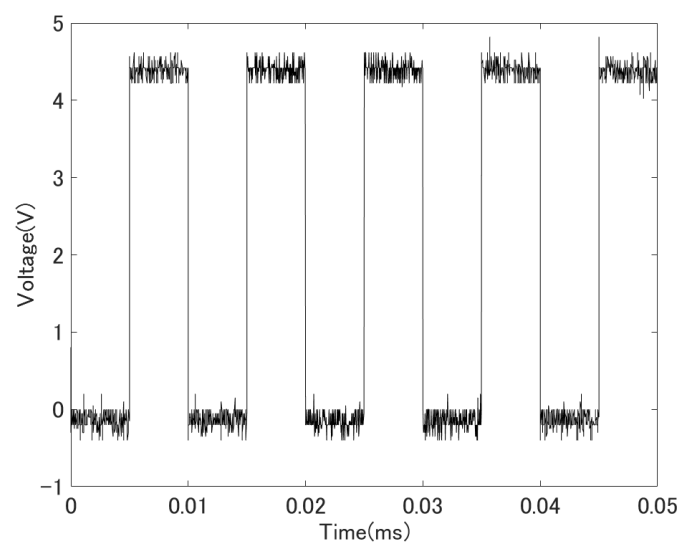


図 3.10 評価用ターゲット信号

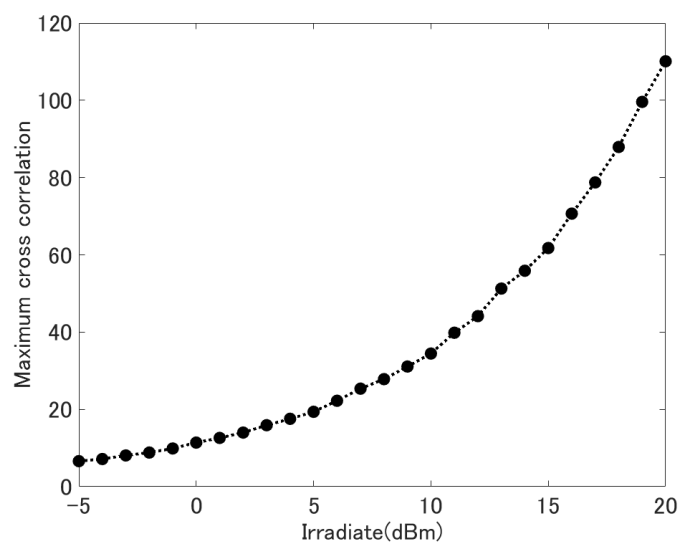


図 3.11 照射強度と相互相関の最大値の関係

3.4 提案手法の脅威の考察

本節では、提案手法の脅威について攻撃のコストと対象機器範囲の観点からの考察を行う。攻撃の実行性については、絶対的な評価が困難である為、従来の機器からの漏えい電磁波による情報漏えいの脅威との比較を行い、相対的に評価を行う。

3.4.1 攻撃コストの考察

本項では攻撃のコストを機材と攻撃パラメタの調査の面から評価を考察する。

従来の機材のコストは、図 3.2 に示すように受信アンテナと、スペクトラムアナライザや SDR のような AM 復調機で構成される。提案手法では従来のセットアップに加えて、電磁照射を行うセットアップが必要となる。これは搬送波として注入する信号を生成するシグナルジェネレータと、信号を電磁波として送信するためのアンテナで構成される。本研究では照射電磁波の強度を正確に制御するためにシグナルジェネレータを用いたが、SDR などでも代用が可能である。

攻撃パラメタ調査の面では、従来の攻撃では漏えい電磁波の強い場所やその周波数、ターゲット情報を再構築するためにターゲット情報のプロトコルについて調査を行う必要がある。一方、提案手法では、漏えいを誘発する構造の特定と、漏えいを誘発する構造へ搬送波を注入可能な周波数を調査する必要がある。漏えいを誘発する構造の特定の方法は 2.2 節で述べたように公開情報から推定が可能である。注入する周波数の調査方法について、本研究では注入する周波数は漏えい電磁波の周波数を調査したうえで決定したが、攻撃を実行するのみであれば、ターゲット機器へ電磁波を照射し周波数スペクトル上で側帯波が生ずるかを、照射周波数をスイープしながら測定することで周波数が特定できる。

以上から、従来の攻撃より多くの機材が必要となりコストが大きくなると考えられる。パラメタ特定の面では、調査の内容が異なるため直接的な比較は困難である。しかし、漏えいしている電磁波の中にターゲット信号が含まれているかの判断においては、従来の漏えいではターゲット情報によっては復調を行うまでは判断が困難となる一方、提案手法では AM 変調のスペクトルがみられるため、注

入周波数と側帯波の差から漏えいしている情報の周波数が分かるため、判断が可能となり、パラメタ特定にかかる調査のコストが小さくなると考えられる。

3.4.2 攻撃対象の範囲の考察

本論文では、情報漏えいを誘発する構造が存在している機器に対しての脅威を提案した。ただし機器からの漏えいが確認されている機器のすべてに適用できるかという点は、更なる検討を行う必要がある。

一方で、3.3.2 節の結果からも、機器からの漏えい電磁波の放射が微弱で、従来の手法で攻撃を行うには大きなコストを要していた機器に対しては、低いコストで攻撃が実行できる可能性がある。

距離に関しては提案手法を用いることで、漏えいの強度が増大するため、より遠方から攻撃を行える可能性がある。複数の機器への攻撃は、同一の周波数で注入可能である場合、漏えいが同時に発生する。ターゲット情報の周波数が異なる場合は、それぞれの分離が容易であると考えられるため、同時に情報が取得できると考えられる。また、ターゲット情報の周波数が類似している場合は、指向性が強いアンテナを受信に用いることで、強度の差が発生するため分離が可能となる。

以上のことから、従来の脅威と比較して、必要な機材は多くなるが、漏えいを誘発する構造が存在している機器に対しては、従来の脅威の対象外となっていた機器に対しても攻撃が行えるため、より大きな脅威となると考えられる。

3.5 対策に関する検討

本節では、提案手法に対する対策の検討を行う。

1.1 節で述べた従来の機器からの漏えい電磁波に対する対策は、提案手法においても有効であると考えられる。しかし、3.3 節の結果から電磁照射の強度により漏えい電磁波の強度が、機器由来の漏えい電磁波の放射強度より大きくなる場合があるため、従来の対策をより高い水準で講じる必要がある。また、電磁照射を受けても、誘発される漏えい電磁波の強度を最低限に抑えるため、機器の電磁

妨害耐性(イミュニティ)を、故障・誤作動を引き起こさないことを目的に勧告されているレベルよりも高く確保することが有効であると考えられる。

4. 結論

本論文では、機器からの漏えい電磁波が観測されないため、従来の電磁波を介した情報漏えいの脅威の対象ではなかった機器にも適応可能な、漏えい電磁波を誘発する手法を提案し、評価を行った。

第2章では、提案手法による漏えい電磁波の誘発の原理と、そのような漏えいを引き起こしうる構造を示した。また、攻撃者がこうした構造を、公開情報を基に推定できることを示した。そして、漏えいの発生を実験で確認するために、2台のマイクロコントローラを有線接続し、デジタル通信環境を模擬した実験環境を構築した。

第3章では、実験を通じて電磁照射により従来とは異なる漏えいが発生することを、機器からの漏えい電磁波の復調信号との比較や、電磁波の照射時、非照射時の復調波形を比較し、照射時のみ情報が漏えいすることから示した。また、照射強度による情報が含まれる側帯波の強度の変化や、漏えい電磁波の復調信号とターゲット信号との相関値を用いた評価を行い、電磁照射の強度が高いほど復調信号がターゲット信号に類似することを明らかにし、照射強度が強いほどターゲット信号に忠実な信号が復元できることを示した。この結果より、照射強度を変化させることで、攻撃可能な距離を制御できることを示した。また従来手法との比較を行い提案手法の脅威について考察を行い、本手法への対策を検討した。

謝辞

末筆ながら、本研究を行うにあたり、ご支援下さった皆様に深く感謝の意を表します。

本学林優一教授には、日頃の研究活動において懇切丁寧なご指導を賜りました。ここに心より御礼申し上げます。

本学藤川和利教授及び安本慶一教授には、研究を進めるにあたり有益なご助言・ご討論を戴き、心より御礼申し上げます。

本学藤本大介助教には、本研学生活の中でご助言とご支援を戴きました。厚く御礼申し上げます。

仙台高等専門学校衣川昌宏助教には、研究活動から論文の執筆に至るまで様々なご助言を戴きました。厚く御礼申し上げます。

最後に、日ごろの研学生活において様々な面でご協力いただきました、研究室の皆様がこの場を借りて深く感謝申し上げます。

参考文献

- [1] Wim van Eck, "Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?," *Computers & Security*, Vol.4, pp. 269–286, 1985.
- [2] Markus Guenther Kuhn, "Compromising emanations: eavesdropping risks of computer displays," University of Cambridge Computer Laboratory, Technical Report, UCAM-CL-TR-577, 2003.
- [3] Martin Vuagnoux and Sylvain Pasini, "An Improved Technique to Discover Compromising Electromagnetic Emanations," in *Proc. 2010 IEEE Int. Symp. EMC*, pp. 121-126
- [4] 登坂俊英, 山中幸雄, 福永 香, 服部光男, "プリンタから漏洩する電磁波に基づく印字情報再現性の評価," 平 20 電学全大シンポジウム, no.1-S2-7, 2008-03.
- [5] Markus Guenther Kuhn, "Security Limits for Compromising Emanations," *Lecture Notes in Computer Science*, CHES2005, vol. 3659, pp. 265-279, Aug 2005.
- [6] International Telecommunication Union-Telecommunication Standardization Sector(ITU-T), "K.84: Test methods and guide against information leaks through unintentional electromagnetic emissions," 2011.
- [7] International Telecommunication Union-Telecommunication Standardization Sector(ITU-T), "K.115: Mitigation methods against electromagnetic security threats," 2015.
- [8] Cypress Semiconductor Corporation, "PSoC 4200L Family PSoC 4 Architecture Technical Reference Manual(TRM).pdf,"
<https://www.cypress.com/documentation/technical-reference-manuals/psoc-4200l-family-psoc-4-architecture-technical-reference>